SEPTEMBER 2001

Federal PROBATION

a journal of correctional philosophy and practice

SPECIAL ISSUE ON TECHNOLOGY AND CORRECTIONS:

Federal PROBATION

a journal of correctional philosophy and practice

PUBLISHED BY
The Administrative Office of the United States Courts

Leonidas Ralph Mecham, *Director*

John M. Hughes, *Chief*
Federal Corrections and Supervision Division

Federal Probation ISSN 0014-9128 is dedicated to informing its readers about current thought, research, and practice in corrections and criminal justice. The journal welcomes the contributions of persons who work with or study juvenile and adult offenders and invites authors to submit articles describing experience or significant findings regarding the prevention and control of delinquency and crime. A style sheet is available from the editor.

Federal Probation is published three times yearly, in June, September, and December. Permission to quote is granted on the condition that appropriate credit is given the author and *Federal Probation*. For information about reprinting articles, please contact the editor.

Subscriptions to *Federal Probation* are available from the Superintendent of Documents at an annual rate of $14.00 ($17.50 foreign). Please see the subscription order form on the last page of this issue for more information.

EDITORIAL STAFF

Timothy P. Cadigan, *Executive Editor*
Ellen Wilson Fielding, *Editor*
Janice G. Barbour, *Editorial Secretary*

Federal Probation
Administrative Office of the U.S. Courts
Washington, DC 20544
telephone: 202-502-1600
fax: 202-502-1677

Postmaster: Please send address changes to the editor at the address above.

Foreword

IN LIGHT OF the ever-increasing role of technology in the field of community corrections, we concluded that a special issue of *Federal Probation* devoted to this topic would be an appropriate way of bringing together some of the many issues and changes that have resulted from this evolution. Our goal was to try and cover as many of the potential issues as possible, while recognizing that we could not cover them all. We hope you find this special edition useful in making the transitions necessary to accommodate the rising impact of technology on our field.

It was only 12 years ago that the first 100 computers were purchased for probation offices in the federal system. From humble beginnings we have come a long way. Today the federal probation and pretrial services system is totally networked, has more computers than we have personnel, has begun to implement a state-of-the-market case management system and is exploring the possibilities of a variety of new technologies, including handheld computers, global positioning systems, geographic information systems, electronic kiosks, voice recognition and computer telephony. While much has been done, there is still so much to do and we look forward to working together to continue to use technology to make the criminal justice system more effective and efficient.

This special edition of *Federal Probation* focuses on technology, but it also makes a concerted effort to provide the reader with an officer's or practitioner's focus. We believe that the reality of these technological changes warrants that focus and we have called on several members of our own community to provide that direction.

This is an exciting time, with so many promising technologies emerging that it is easy to get swept up in the technology and forget that the primary mission of community corrections is to investigate and supervise defendants and offenders while providing for the safety of the public. In addition, we need to remember that the significant changes we are undergoing make their own demands on the staff of the federal system, who need the necessary training and support to utilize the tools we give them and minimize the negative impacts of change on them.

Timothy P. Cadigan
Executive Editor, *Federal Probation*

THIS ISSUE IN BRIEF

DEPARTMENTS

Technology Forecast for the Federal Judiciary

Office of Information Technology
Administrative Office of the U.S. Courts

FORECASTING TECHNOLOGY, in particular forecasting information technology, can be problematic. The difficulty is that the ebb and flow of information technology is regularly interrupted by episodes of paradigm disruption. The introduction of personal computers, the World Wide Web, and cellular communications are episodes that lifted technology from one track and dropped it clumsily on another. This paper treads on safer ground . . . it focuses on more predictable aspects of technology . . . it avoids forecasting the 'whiz-bang' and makes a wide path around consumer electronics. This paper reviews major trends that represent opportunities for the judiciary—opportunities to invest in and exploit technology to improve business processes. A complement to the Long Range Plan for Information Technology in the Federal Judiciary, it addresses the future. As a result, some technologies discussed are not quite ready for implementation but will likely play a lead role on the three- to five-year planning horizon.

This paper organizes technology trends into five categories: networking, security, the "people factor," information management, and standards. All five categories share some clear similarities:

- The undeniable influence of the Internet. The Internet—perhaps the most significant force in the future of information technology—has dramatic effects on product development and on the ways in which people perceive information systems. Indeed, the sudden, explosive, growth of the Internet has moved the discussion from "if we use it" to "how we use it." The Internet is firmly entrenched in the present: it is here, it is now, it is ubiquitous.
- A change in attitudes about technology, both in the private sector and in the government. Technology consumers used to be concerned only with requirements: "How can we meet our current needs with technology?" It is now common knowledge that technology developments may offer previously unforeseen opportunities, and concerns have changed to "How can we exploit technological developments to improve our business processes?"
- Information technology (IT) as a necessary infrastructure for doing business. No longer just a curiosity or a typewriter surrogate, computers have infiltrated all business processes, and the quality of these processes depends upon reliable, well-planned computer systems.

The judiciary has generally adopted a "state-of-the-market" strategy to guide IT investment decisions. This is a safe strategy that avoids the risks encountered by more aggressive "early-adopters" (those who invest in technology as soon as it becomes available—before its value is proven and limitations are shown). There are several notable exceptions to this rule where the judiciary has opted to be an early-adopter in order to take advantage of the extraordinary benefits obtainable by some new (and admittedly risky) technology. The judiciary has mitigated the risk by prototyping the technology before committing to it. Either strategy buys some breathing room for the technology forecaster. Whether current or future, the IT market can be fickle. Even investment decisions based on the state of the market are best made with an eye toward the future in an attempt to project whether the current state is a stable state. And that is the principal charter for this technology forecast.

The remainder of this paper presents major trends, impacts on the federal judiciary, and possible courses of action for each major trend along with links to the following 2000 IRM strategic initiatives:

- Implement electronic libraries to enhance desktop access to a variety of electronic research tools and databases.
- Modernize case management through the use of state-of-the-market technology and refined business processes, such as electronic case files systems.
- Use video telecommunications technologies to facilitate more efficient training, conferencing, administration, and judicial proceedings.
- Employ technologies to improve the quality and efficiency of courtroom proceedings.
- Use the Internet and judiciary intranet on the judiciary's DCN to make publications, information, and services more accessible within the judiciary and to the public.
- Implement the strengthened post-automation review program.

Networking

Network computing architecture and the Next Generation Internet represent two

This report is part of the 2001 update to the Long Range Plan approved by the Judicial Conference of the United States.

strong trends that place the data network as the fundamental building block for implementing new information technology.

More than a decade ago, Scott McNealy (CEO of Sun Microsystems) said, "The network is the computer." Although it took a long time to happen, it was a prescient forecast. Perhaps the ultimate embodiment of this thinking is the current trend toward "network computing architectures." There are two main underlying concepts: 1) the thin-client, a stripped-down, desktop personal computer which depends on the network for computing and storage resources, and 2) the network appliance, a special purpose computer that does one thing well.

The thin-client trend addresses a significant problem in information systems: the cost of owning and maintaining PCs. For the consumer, purchasing a PC can cause even more dissatisfaction than buying a car—within a year of purchase, a PC is obsolete. New software products require more processing speed, more memory, and more disk space. It becomes increasingly difficult to run new software releases and take advantage of improved technology with a one-year-old museum piece.

This cost/obsolescence problem is amplified when the PC is part of a business environment. The new hardware purchase price is dwarfed by the cost of maintenance and operation. These costs have been termed "total cost of ownership," or "TCO." TCO includes the salaries of the systems administrators and technicians who must visit each PC, perform routine and emergency maintenance on hardware and software, keep track of how users have customized their PCs to personal preferences, and make sure the PC can continue to run applications such as case management.

The biggest benefit of a thin-client architecture is that it reduces reliance on the desktop computer by moving software and data onto the network. The support costs for a thin-client are reduced because the software for all thin-client PCs are installed on the network in one place, once, for all PCs. A thin-client PC will also have a longer usable life because it relies on the network for the computing and storage resources required to run the latest programs. The downside of a thin-client strategy is the increased reliance on the network for performing basic functions such as word processing and spreadsheet activity—if the network is down, the user is down.

One extreme version of the thin client is the network computer (or NC). Network computers are PCs with no local disk storage, but with a fast connection to the network. All programs and data are downloaded from the network as they are needed. Early enthusiasm for network computers has waned greatly, but the TCO savings potential of the network computing architecture means that many organizations will be looking for ways to exploit some variation of thin-client technology in their information systems. Perhaps hand-held computers (e.g. the Palm Pilot), which by their very essence are thin, will replace the NC.

Filling the enthusiasm gap are network appliances. Network appliances run the gamut from toasters and door-knobs[1] to massive super-computers. The common theme is a standalone device that can be attached to a network. In practice, most interest is focused on devices that deliver service-level applications (like a database or web servers). Since thin-clients only see services on the network and never the operating systems on the computer that provide the service, the application can run on raw iron, a computer with no operating system, or on a computer with a special-purpose operating system. An application running on raw iron is expected to be faster and less expensive than an application running on a general purpose computer. Time will tell.

Greater reliance on networks will require that investments be made in building reliability and bandwidth. The Next Generation Internet (NGI) and Internet2 (I2) projects—part of a federally, academically, and industrially supported research and development program—illustrates the widespread recognition of the importance of investing in networks.

NGI's objectives include making a quantum leap in the capacity delivered to Internet users. NGI plans to bring 100 times the typical Internet data transfer speeds to 100 pilot sites, and they plan to bring 1,000 times the speed to 10 pilot sites. The NGI vision is to "provide a powerful and versatile environment for business, education, culture, and entertainment. Sight, sound, and even touch will be integrated through powerful computers, displays, and networks."[2]

NGI, as it grows, will reformulate the public's concept of what can be accomplished over a network. For example, a network environment such as NGI would accommodate widespread deployment of videoconferencing with capacity to spare.

The judiciary will be affected by pressures to reduce total cost of ownership and increase the data communications speeds offered by the Data Communications Network (DCN) and other networking services.

The judiciary can reap some TCO benefits from the trend toward network computing web work browsers, such as Netscape Navigator and Microsoft Internet Explorer, as the user interface. This strategy keeps the PC (or the client) thin. It reduces the amount of software needed locally on the PC and establishes a common, familiar interface to applications—a sensible near-term step for the judiciary to take while keeping an eye on the progress of network computing over the next few years. A gradual "thinning" of the client can reduce the PC management burden and cost and still use existing equipment and software.

Regardless of the success of network computing, projects such as NGI indicate that there will be growing pressure to improve the reliability and increase the data transfer capacity of networks. One of the judiciary's IT strategic initiatives explicitly identifies increased use of Internet, intranet, and DCN services to make information more accessible. The visionaries behind NGI realize that improving networking infrastructure is an ambitious undertaking that should be started small and then grown. This approach also makes sense for the judiciary's network infrastructure.

Security

The need to protect credit card purchases on the Web has advanced two important information security technologies: identification and authentication (I&A), and encryption. Information security did not carry widespread audience appeal until people started buying merchandise on the Web. A simple credit card purchase over the Web invokes sophisticated identification and authentication (I&A) and encryption technologies and algorithms. Web consumers have come to trust this technology to protect their credit card numbers as they are being broadcast over the Internet. I&A includes a wide array of techniques used to prove to two parties that each is who they claim to be—in the case of electronic commerce, that the consumer is the actual credit card owner and that the Web site is run by a legitimate merchant.

More generally, I&A is the fundamental first step in maintaining the security of any general-purpose information system. The information system must confirm that its users are who they say they are and grant access privileges accordingly. Advances in both I&A and cryptography have introduced many new security tools to make it easier on the user while also protecting information resources:

- **Single log-on.** Password protection is the most common way to implement security. Typically, users are asked to remember

multiple passwords and are encouraged to change them frequently. This results in users selecting simple, easily guessed passwords, and diminishes the strength of password protection. Single log-on technology allows users to enter a password once and gain access to all systems for which they have privileges.

- **Biometrics.** Biometric I&A relies on a unique physical characteristic of the information system user: a fingerprint, a retinal image, a voice. Devices that can reliably read fingerprints are affordable and virtually eliminate the need to memorize and manage passwords.
- **Smart cards and one-time passwords.** A smart card looks like a credit card but has an embedded computer chip. Smart cards have many uses, but one of the most interesting security-related uses is to generate one-time passwords. A one-time password is time-sensitive and can be used only once. Even if it is "sniffed" (i.e., intercepted by an electronic eavesdropper), it cannot be reused.
- **Public key cryptography**. Traditional cryptography uses a single, secret key to encrypt (scramble) information to protect privacy and to decrypt (unscramble) the protected information. Communicating parties must somehow share knowledge of the secret key. Public key cryptography uses key pairs: a private key, known only to the individual user, and a public key, published for all to know. Messages encrypted with the private key can only be decrypted with the public key, and vice versa.

This concept is very useful. If Bob has a message that he wants only Alice to read, he can encrypt it with Alice's public key. If Alice wants to digitally sign a message so that Bob can confirm that it came from her and her alone, she can encrypt it with her private key—only her public key will make sense out of it.

The judiciary's 2000 IRM strategic initiatives will result in increased information accessibility, increased exposure, and increased risk of a security breach. To be effective in mitigating this risk, security must be applied consistently, and security tools must be easy to use.

The technology is available to ensure the protection and integrity of sensitive court documents and information. Information security is an area in which the application and management of the technology is the primary challenge. The judiciary is moving forward on some of the following information security fronts and may wish to explore some of the most recent technologies:

- Implement a consistent security architecture and policy. The information security chain is as strong as its weakest link. A consistent architecture and set of policies for protecting information will provide the most important security tool: uniform implementation of technology and procedures to safeguard sensitive information. The judiciary has begun this effort.
- Implement a Public Key Infrastructure. Public key cryptography offers essential tools to protect information and ensure integrity; they are used for both authentication and encryption. The organizational structure required to manage public keys is called a Public Key Infrastructure, or PKI. The PKI will have to address policy issues such as the escrow of public keys used for encryption.
- Explore I&A tools that make it easy for the user to follow security guidelines. Many of the new security tools, particularly biometrics and smart cards, are aimed at improving protection while reducing the user's burden. The judiciary is currently evaluating several of these tools.

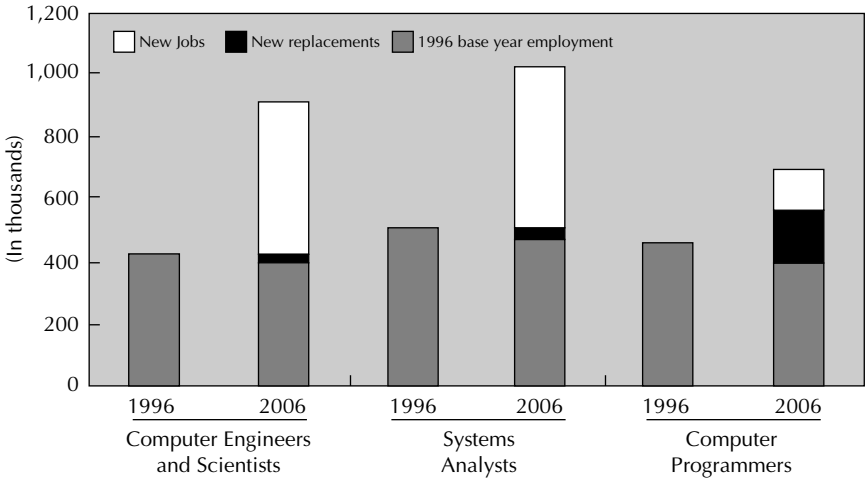
The People Factor

The people factor is more significant than most technologists allow and may be the limiting factor in determining how completely and how quickly new technology can be effectively deployed. The growing role of information technology in nearly every business sector will increase the need for trained, skilled staff at all levels. Figure 1 projects a near doubling of the demand for skills in the key IT disciplines, and there are indications that supply will not keep pace with demand. For example, the years 1985 through 1997 saw a 16 percent drop in the number of students graduating with bachelor of engineering degrees. From 1985 to 1996, there was a 29 percent drop in math and computer science graduates and a 42 percent drop in information system bachelor degree recipients.[3] (See Figure 1)

The next decade will see a high demand for IT skills. While sources of information systems development and operations skills are decreasing, the needs and expectations of the information worker are increasing. The judiciary's IRM strategic initiatives to modernize case management, employ technologies to improve the quality of courtroom proceedings, and increase information accessibility will require skilled IT system development and operations staff, and it appears likely that these skills will be in short supply through the next decade. The judiciary will be called upon to focus increasingly on internal training to improve staff skills in IT disciplines and tools. In addition, it will become increasingly necessary to take advantage of the economies of scale in stretching available expertise over a wider range of courts with similar needs.

As the information audience grows, more accommodations must be made for the disabled and the aged. As the designers and implementers of judiciary information sys-

FIGURE 1:
Projected Growth of IT Professions



Source: Bureau of Labor Statistics, U.S. Department of Labor, 1996

tems begin providing greater accessibility to a wider audience through electronic media, they will need to consider the broad spectrum of that audience's needs. Americans with disabilities may have sight or motor skill impairments that prevent them from accessing information presented through Web pages or other electronic means. Aging Americans may also have limitations.

Emerging presentation and programming technologies and products address the need that visually impaired, hearing impaired, and motor-skill impaired Americans have to access public information maintained by a court computer system. Current interactive voice response (IVR) systems such as the Appellate Voice Information System (AVIS) and the Bankruptcy Voice Case Information System (VCIS) are examples of positive steps being taken in this direction.

Information Management

The growing volume of information from the Internet, intranets, and online libraries is overwhelming. The issues surrounding the management of information—extending beyond the technology itself—are critical to using the power of information accessibility to improve court processes.

Access to information is no longer the challenge; the new challenge is to find information and use it effectively. On the Internet, for example, an entire industry has grown around "portal" Web sites (e.g., Yahoo! and America Online) that provide search engines to find and place a temporary, rudimentary organizational structure around information. Recognizing that information known only to one person is of limited use, software products, loosely labeled GroupWare, provide tools to refine the organization of information and share it.

The judiciary currently employs three GroupWare tools: electronic mail, videoconferencing, and the Intranet. Other more sophisticated tools implement document management, workflow management to automate business process flows, and collaborative tools to allow judges, attorneys, clerks, probation and pre-trial officers, and staff to interact and share information electronically.

Workflow management products are fairly mature and provide a good example of GroupWare beyond the basic office tools. Workflow tools automate the movement of information through one or more business processes during which documents, information, or tasks are passed from one participant to another for action, according to a set of defined procedural rules. The step-by-step processing of a court case according to the Federal Rules of Procedure and local district rules is an example of a workflow.

Automated workflow systems were initially designed to increase productivity in processing high-volume, repetitive transactions. In addition to accelerating processing times, workflow can also improve collaboration, increase adherence to procedures, and reduce the routing of paper documents. Workflow tools in a court environment could help to reduce administrative tasks such as monitoring calendars, ensuring that responses are received at the proper time, that hearings are promptly held, that orders are issued on time and, in general, that the work of the court efficiently moves in the proper sequence. The court's administrative staff and the judges can then spend more time on the delivery of justice and less time recording and monitoring the process of justice.

There is an overwhelming need to use GroupWare and knowledge-based technology to better manage information. The judiciary's experience with the J-Net Intranet site has revealed the importance of policy-related issues in information management:

- *Data Ownership and Information Maintenance.* Electronic publishing gives life to information and documents. Those that access the information electronically expect it to be up-to-date and accurate. This raises a host of policy questions and challenges such as who "owns" the information? Who can authorize updates? What is the responsibility of the owner for maintaining currency?

- *Electronic Records Management.* A recent decision of the Court of Appeals for the D.C. Circuit identified electronic records that were subject to the provisions of the Federal Records Act. The decision resulted in the issuance of an IRM bulletin stating that "The Court found that the paper copy of an electronic message might not include all of the information that the electronic record contained and thus was not a duplicate record." This means that a subset of electronic records must now be handled and managed as formal federal documents. Policies and procedures must be established that apply to many electronic records including some e-mail previously considered to be transient and disposable.

- *Privacy.* Although there is already the need to set policy on what information is available to the public, publishing electronically adds complexity. By increasing the ease of access and the scope of exposure, electronic publishing represents an increased level of public availability and potential violation of personal privacy. In cases where information access is only provided to a subset of authorized individuals, reliable technology must be in place to enforce access policy. Technologists must become aware of privacy needs, and policy makers must become aware of the capabilities and limitation of information security technology. The judiciary must also be aware that commercial resellers of judiciary information may not have the same privacy concerns that the judiciary has.

Although answers to these questions are not all technological, technology can help in implementing information management policy as it is developed. For example, GroupWare products are beginning to include Intranet and Web site management tools to implement ownership and maintenance policies.

The public has begun to trust the Internet for conducting commerce and now sees its convenience and efficiency. Many court transactions can take advantage of electronic commerce (EC) technologies.

It is estimated that more than 12 million consumers purchased merchandise over the Internet in 1997. By 2002, the number of consumers is expected to increase by a factor of five and their individual spending to increase by 400 percent.[4] If there ever was a phobia about conducting commerce electronically, it seems to be passing.

For the same reasons that consumers have been drawn to Internet shopping—convenience, efficiency, and value—the judiciary may wish to consider EC for conducting a wide variety of transactions including filing fees, fines, restitution payments, court costs, and reimbursement for public defender services. Not all EC transactions are necessarily financial transactions. Electronic filing of court documents is an important technology that also falls into this category. The CM/ECF project already offers electronic filing as part of its first release, and is exploring fee collection over the Internet for a future release. As the judiciary has learned with electronic document filing, security and reliability are fundamental issues to the success of EC. The maturity of technologies to ensure that, for example, credit card numbers remain pro-

tected in a consumer purchase, can be applied to protect court transactions as well.

Standards

The Internet has fortified standards and created real tools for exchanging electronic information between business partners. Insistence on standards will add longevity to technology, improve interoperability, and increase flexibility in product selection.

When it comes to standards, the Internet is the benchmark. The Internet has become a final testing ground for most information system standards. It has created real working standards out of many previous paper-only standards.

Perhaps the biggest success story is the Transmission Control Protocol/Internet Protocol (TCP/IP) standard—the workhorse protocol that provides basic connectivity for the 50 million or so computers that interoperate on the Internet. The protocol was originally adopted in 1982, and it is estimated that a new version will not be needed until 2015. Other standards have evolved into valuable interoperability tools: Simple Mail Transfer Protocol (SMTP) allows universal e-mail connectivity, and the worldwide web protocols (HTTP and HTML) allow users to access all kinds of data from all kinds of computers from anywhere in the world.

There are lessons to be learned from the success of these standards:

- *Permanence.* Standards compliance reduces product dependence and product obsolescence. For example, documents that must be available for many years in the future should not be stored in proprietary formats.
- *Interoperability.* Strategic initiatives to automate case management and court proceedings require that a large group of "trading partners"—both internal and external to the judiciary—exchange information. For this exchange to happen, the form and structure of that information must be standardized.
- *Increased competition and vendor independence.* Adherence to standards reduces reliance on a single vendor for important technological tools and provides the added financial benefit of increased competition among suppliers.
- *Business benefits.* The benefits of IT industry standards may be extended into business-specific areas of the judiciary. E-mail naming conventions are a simple example of how internal standards could improve interoperability within the judiciary.

Unfortunately, there are some drawbacks to information systems standards. Although there are many mature, well-subscribed standards, compliance with standards is not always viewed by product vendors as being in their best interest. Many vendors—in some cases, influential vendors—work very hard to differentiate themselves by adding nonstandard bells and whistles to their products. In general, a practical information system strategy favors standards wherever possible, but recognizes that in some cases a product-based standard may be necessary.

Parting Words

This is the second year that the Long Range Plan for Information Technology in the Federal Judiciary has included a technology forecast—a clear, and now consistent, signal that the federal judiciary recognizes the importance of technology trends and direction in their plans for future information systems. Although network computers have been depreciated and network appliances have been added, there have been relatively few changes. One year is not much of an interval when the future is concerned. This paper opened with a charter to identify technology developments that can improve judiciary business processes and maintain an eye toward potential future states of the market. Technology offers more opportunities than we probably care to have. Even the capabilities of current technology stretch our ability to manage information and processes.

In addition, any investment decision, technological or otherwise, must be tempered by available funding. The future challenge will be to make sure policy and management practices mature to keep pace with rapid technological advances and to deploy IT products that produce real benefits. For many of the trends described in this forecast, the true challenge is the management of technology.

Endnotes

[1] Both devices actually exist and, at least in the latter case, are useful. Controlled from the network, the door knob can report who uses it and can be set with different security profiles and keys.

[2] NGI Concept Paper. (1997, July). Retrieved November 20, 1998 from http://www.ngi.gov/concept-Jul97/.

[3] Sweat, Jeff. (1998, April 10). TechWeb. *IT Hiring Shoots Up While Tech Graduates Decline.* Retrieved November 20, 1998 from http://www.techweb.com/wire/story/TWB199804410S0009.

[4] Consumer Internet—The U.S. and Worldwide Forecast for Consumer Internet Usage and Commerce. IDC/Link (1998, March).

Supervising the Cyber Criminal

Brian J. Kelly
Senior U.S. Probation Officer and Cybercrime Specialist

ENACTED IN 1986 and amended several times since then, 18 USC 1030, the Computer Fraud and Abuse Act, is the primary criminal statute used for prosecuting fraud and related activity in connection with computers. This statute covers those who knowingly and/or intentionally access a computer(s) and obtain information they were not authorized to have access to.

As the world of computers and cyberspace becomes more and more ingrained into our daily lives, so will cybercrime. Increased prosecution of cybercrime will mean, for United States probation officers, preparing for the special demands of efficiently investigating and supervising these offenders and providing the court with understandable and accurate information about them.

First, who is the cybercriminal? He or she is not simply the lone juvenile hacker using a Christmas present from Mom and Dad. Cybercriminals come in all forms, from the street drug dealer to the identity theft mastermind. Many people place in this group the sexual predator who makes use of a computer for child pornography and solicitation. In my opinion, these offenders belong in a different category from those we are discussing in this article. Sexual predators' computer use is secondary; their problem is deeper rooted. Take away sex offenders' computers and they will, if they have not already, find other ways of luring children, distributing and receiving child pornography, etc. The focus of the supervision of the sex offender should be the offender's mental state and ability to carry out desires. (Sex offender and cybercrime specialists will, however, have much in common and are likely to work in tandem at times as cyberspace increasingly becomes the means of choice by sex offenders.)

The cybercriminal can be defined as someone whose knowledge and use of computers and/or the Internet has enabled him or her to commit the crime of choice. This definition covers everyone from the first-time offender whose spontaneous hack into a former employer's database is based on revenge to hacker/crackers such as Kevin Mitnick, who have a long list of computer-related offenses and whose instant offense is the culmination of criminal activity covering a period of months or even years, spanning intrusion into classified military information to obtaining free telephone service.

The Pre-Sentence Interview and Report

The first duty of the United States Probation Department is the preparation of the Pre-Sentence Report, which contains a sentencing recommendation to the court. For the cybercriminal, the PSR must contain a clear and precise offense conduct section explaining the motive and means of the offense. The court and, eventually, the supervision officer determine the offender's computer knowledge and motive for participation in the offense. The motive may be purely financial (intrusion into an e-commerce web site to steal customer information, for example), anger (denial of service attack on a former employer), or extortion (intrusion into an e-commerce web site to steal information to use to extort the company instead of further criminal use). The report should also accurately describe the computer equipment owned by the offender. Most important, the report carries a sentencing recommendation to the court. This recommendation must include specific special conditions covering the offender's computer and Internet usage. How restrictive these special conditions should be is based on the severity of the instant offense and the offender's criminal history. For example, a first-time offender who has committed an isolated denial of service attack against a former employer may not warrant a full prohibition from computers and/or the Internet but rather a condition prohibiting any contact, including computer contact, with the former employer, as well as employer notification if the offender plans to obtain employment within the computer industry.

The Eastern District of New York Probation Department has recently issued a Bench Guide to the Judges of the district which includes the classification and wording of special conditions. The following are a few of the special conditions listed under the section titled "Cybercrime (Computer/Internet)":

- The defendant is not permitted to access a computer or a connected device (except a land line telephone) at any time.
- The defendant is not permitted to access the Intranet/Internet or bulletin board systems at any time.
- The defendant is not permitted to engage in the use of encryption.

Other special conditions should also be considered in these cases; for example, restitution for any damages caused by the offender, mental health treatment for anger management, search and seizure condition, etc.

Supervision Methods

Effective supervision of the cybercriminal need not be limited by the level of computer knowledge and skill of the officer. In fact, only a small percentage of the supervision of the cybercriminal will involve advanced computer knowledge. The majority of the supervision will combine traditional and non-traditional supervision methods with a level of computer knowledge consistent with regular use of a computer and the Internet. Considering the influx of computers into our professional and personal lives, this is not a steep hill to climb.

Officers supervising cybercriminals, and especially those who need to enforce cyber-specific special conditions, should become familiar with various methods that can assure full compliance and detection of non-compliance.

The Initial Interview

Using the pre-sentence report as a background, the cybercriminal should be interviewed with the same goal as with any other offender—that is, to obtain as much relevant information as possible. For cyber-specific information, the officer should attempt to gather two groups of information, addressing ability and means. Under the category of ability, how complex was the instant offense? What formal computer education/training has the offender had? How long has the offender been employed in the computer industry? As for means, what computer equipment does the offender own or have access to? Who are the offender's Internet Service Providers (ISPs)? What are the offender's email addresses/screen names? As previously stated, the pre-sentence report should contain a full listing of the offender's educational and employment history, as well as asset information.

In the Eastern District of New York, we have compiled a Computer/Internet Data Sheet for the offender to complete and return to the supervising officer. This Data Sheet contains questions about hardware, software, and Internet accessibility and use.

The Home Contact

As with any offender, the home contact is the most valuable supervision method, because it offers the officer an insight into the daily life of the offender. With the cybercriminal, the focus will mainly be on the computer workstation. Any evidence of non-compliance will most likely be found in this area. The officer should be familiar with the hardware the offender has reported he owns or has access to (*Computer/Internet Data Sheet*). Any hardware not listed or recently obtained should be recognized by the officer. The officer should be aware of any print-outs or notes in plain view around the work station. If the computer is on, the officer can note the software that may be running and other programs on the system by simply looking at the screen. During the home contact, the officer should also notice other connected devices, such as laptop computers, personal data assistants (PDAs, i.e. Palm Pilot), cellular phones, and pagers. The officer must be sensitive if the offender is living with other members of his/her family, since they may use the computer or other devices.

The Employment Contact

During the employment contact, officers should observe the offender's work area. Does the offender have access to a computer? Does the computer have Internet access? Is the computer networked with other computers? If possible, speak with the offender's supervisor to determine what kind of access the offender's daily duties make possible. The Internet? Other computers? Other databases?

Surveillance

An officer may deem it necessary to verify the daily activities of the offender to assure compliance with special conditions, such as prohibition from accessing the Internet. Surveillance of an offender's visits to locations such as the library, a "Net Café," etc., may indicate the offender is accessing the Internet at locations other than the residence.

Credit Reports and Card Statements, Telephone Records, Mail Covers

An officer should periodically obtain credit reports for the offender and request statements for any active credit cards from the offender. These statements may show charges that would provide insight into the offender's Internet usage, such as an ISP monthly charge, e-commerce purchase, or the like. Telephone records obtained from the offender may reflect calls to ISPs or other databases the offender is accessing with a dial-up modem. Mail covers, which can be requested from the U.S. Postal Inspection Service, can reveal incoming mail from ISPs, online trading accounts (i.e., E-Trade), or credit card companies. Mail covers are particularly useful if the offender is receiving mail using an alias. If warranted, credit card statements and telephone records can be obtained by a court order instead of by requesting the information from the offender.

A recent violation filed in the Eastern District of New York involved an offender obtaining names and social security numbers through stolen mail and using this information to establish fraudulent instant credit accounts online and purchase goods. The offender used his home address, on which a mail cover had been initiated by the officer, and incoming mail showed the names fraudulently used by the offender. This conduct resulted in violation proceedings as well as a new indictment within the district.

Random Hard-Drive Search

If the officer deems it appropriate and necessary, he or she may conduct random hard drive searches of an offender's computer. If no search special condition is in place, the officer must first gain the offender's consent to a search. The search can be as simple as a peripheral search during an unannounced home contact or as complex as physically taking the equipment from the offender and bringing it to a computer forensic lab for analysis. Of course, the removal of equipment from an offender's home or place of business should only take place in an extreme circumstance, where the officer must be prepared to deal with a variety of issues such as chain of custody, privacy laws (if the computer is accessed by other members of the family), etc. But basic peripheral searches that do not involve the removal of equipment, unless evidence of violation or new criminal conduct is uncovered, should be a practice of officers supervising cybercriminals. The following supplies should be on hand if such a search is planned: camera, floppy disks, labels, and note-taking materials. Before conducting a search, the officer should photograph the work station. The search can be done in two ways. First, the officer can enter the hard drive manually, searching folders such as Temporary Internet Files for evidence of Internet use and Notepad or Word documents for evidence of fraud (social security & credit card numbers, etc.). Obviously, this method takes a certain level of computer skill first to access the data and then to preserve it for evidence, if necessary.

If the officer's skill is limited or he/she does not feel comfortable manually searching the hard driver, software is available that will search for certain types of documents. In the Eastern District of New York, the Probation Department has previously used *One Tough Computer Cop,* a program originally designed for parents to monitor their children's computer use. The program is extremely simple to use and requires little computer knowledge.

Essentially, the program searches the hard drive for graphic documents (.bmp, .jpg) and text documents containing key words relating to drugs, violence, gambling, etc. The user can view selected documents easily and quickly. Recently, the company that designed *One Tough Computer Cop* introduced similar software specifically designed for probation and parole officers. EDNY has purchased *Computer Cop Forensi,* which operates on the same premise as *One Tough Computer* Cop but at a much more advanced level. The officer can install the software onto a laptop and via a parallel port cable can view and seize evidence from an offender hard drive while maintaining evidence integrity. This enables searches to take place in the field or in the office if a system is seized. Also used in EDNY are *Internet History Viewer* & *File Rescue.* To find the software that fits your district's particular needs, simply search the web.

During the search, the officer should make notes of any pertinent information, such as software on the hard drive, file information, etc. Once the search is completed, the officer should again photograph the work station.

If the officer deems it necessary to seize the hard drive, labels should be used to identify all hardware and connection ports. An excellent guide to the seizure of electronic equipment, entitled "Best Practices for Seizing Electronic Evidence," is available through a joint project of the International Association of Chiefs of Police and the U.S. Secret Service.

Officers should become familiar with legal issues surrounding the search and seizure of computers and electronic evidence. The Electronic Communications Privacy Act and Privacy Protection Act are two main pieces of legislation that officers should review. As United States probation officers, we have more leeway than other law enforcement agencies, but this should not be used as an excuse to be un- or ill-informed on legal issues surrounding any actions you may be planning to take. The Department of Justice web site on cybercrime (www. cybercrime.gov) contains a wealth of information on cybercrime, including legal statutes and case law.

Monitoring/Recording Software

In current use in sex offender cases are monitoring/recording software programs such as SpectorSoft. This program is installed onto an offender's computer to maintain a photographic record of the computer activity. The officer can randomly access the program and retrieve the data to determine if a violation has occurred or if the program has been tampered with.

Information Databases

The Probation Department currently has access to many information databases, such as Choicepoint, Lexis-Nexis, Westlaw, and SENTRY. All of these databases are extremely useful for obtaining information on offenders. When searching for information about a cybercriminal, officers should be aware of any hacker aliases the offender may have used. Many hackers find the need to brag about their exploits and conquests on message boards, and a random search may uncover such a message. If an offender obtains employment with a company that maintains a web site or claims ownership of a web site, or if the officer uncovers a domain name linked to the offender, the officer may search the **WWWHOIS** database. This database maintains owner information, including addresses and telephone numbers, for most domain names.

Recently, in the Eastern District of New York, an offender claiming to work for an employment agency provided the officer with the company's web site address. The offender, who owes a considerable amount of restitution, claimed to be the office manager, with no ownership interest or ties to the business. A search of the WWWHOIS database via www.network-tools.com revealed that the domain name was owned by the offender's husband and a listed billing address was a former residence of the offender.

Mental Health Evaluation & Treatment

Some cybercriminals are not out for profit but commit the instant offense out of anger, obsession, etc. These offenders should be referred for a psychiatric evaluation to ascertain the necessity for treatment. A spontaneous denial of service attack on a former employer may indicate a deeper anger management issue, while some offenders may have lost touch so completely with reality that they feel the only reality lies within cyberspace. These and other issues may require mental health treatment to prevent a "relapse" into further offense conduct as well as to prepare the offender for a functioning life outside of cyberspace.

The extent to which each of the above methods is used should be decided on a case-by-case basis, considering many factors, especially the restriction level of court-ordered special conditions.

Networking

Federal, state, and local law enforcement agencies have been identifying and addressing the threat of computer-related crime by forming cybercrime investigative units within their agencies. Some agencies have also put together their own computer forensic labs to perform in-house analysis of suspect computer systems. Making contact with these units is essential to the successful supervision of cybercriminals. The High Technology Crime Consortium and New York Electronic Crimes Task Force have put together listservs with Yahoo Groups for law enforcement and private industry professionals involved in the investigation of cybercrime and other technology-related issues. The list of members grows daily and anyone needing assistance in this field is greeted with a wealth of information from members.

Law Enforcement Task Forces are also an excellent way to make contact with other law enforcement professionals and gain assistance in an investigation. The New York Electronic Crimes Task Force coordinated by the U.S. Secret Service combines law enforcement and private industry to help combat cybercrime and other electronic crime.

Conferences such as Cybercrime 2001 Conference & Exhibition, International Conference on Electronic Crime, and Blackhat offer great opportunities to meet professionals in the computer industry and law enforcement professionals specializing in this area. Private companies that participate in these conferences demonstrate software products designed for information security and forensics. Officers should attend these conferences to keep up with the latest software offerings.

Officers should also become aware of legal contacts and subpoena procedures of Internet Service Providers. Obtaining records from ISPs may be the key to an ongoing violation investigation. A list of ISP legal contacts can be obtained at www.infobin.org/cfid/isplist.htm.

The most challenging aspect of cybercrime is the speed of change. Between the composing and publishing of this writing, new products have been released, new web sites formed, new crimes committed. Officers who plan to specialize in cybercrime must be prepared to stay constantly on top of current events. In the Eastern District of New York, cybercrime training has been incorporated into the new officer training program. The training sessions cover topics such as electronic databases, cybercrime special conditions, supervision methods, cybercrime statutes, forms, and media publications. Districts should seriously consider implementing cybercrime training and district policies in the near future to avoid playing a constant game of "catch-up" with the offenders they are supervising.

Cyber Crime and the Courts—Investigating and Supervising the Information Age Offender

Lanny L. Newville
Field Automation Specialist, Western District of Texas

"It should come as no surprise that computer technology is involved in a growing number of crimes. In addition to being used as a tool to perpetrate crimes (e.g., computer intrusion, stalking, harassment, and fraud), computers can contain evidence related to any crime, including homicide and rape. It is no longer sufficient to have a few experts familiar with evidence stored on and transmitted using computers. Any investigation can involve computers or networks and everyone involved in a criminal investigation or prosecution can benefit from knowledge of the associated technical, legal and evidentiary issues related to this technology."

—Eoghan Casey, Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet (Academic Press 2000)

BEFORE THE ADVENT of the Internet and the boom in communications it engendered, computer crimes were fairly localized and the perpetrators were members of a select and secretive group with a high degree of specialized knowledge and skills. The child pornography industry, which had already begun to move from print and film media to computer bulletin board systems, found an open and anonymous home on the Internet with a rapidly growing victim pool. According to Grunwald Associates, a research firm based in California, our children's use of the Internet has increased from 2.3 million in 1994 to 25.4 million in 1999.[1] Unfortunately, preferential sex offenders recognized the apparent advantages of the Internet and were well established before law enforcement became aware of the changes.

The Internet has allowed an explosion of information, both positive and negative. In addition to globalizing adult and child pornography, it has created a venue for the criminally oriented to freely exchange information and provides them with distance-learning opportunities to enhance their illegal skills. It is quite simple to find sites on the World Wide Web where step-by-step instructions for remotely breaking into computer systems, and stealing services such as long distance, and circumventing security measures are openly available. It can also serve as a support system for defendants who are looking for others to validate their behavior.

Those charged with investigating and apprehending violators have found themselves with a huge knowledge deficit. The FBI, U.S. Secret Service, and U.S. Customs have led the field in training investigators and forensic computer specialists. These agencies have made significant progress in their ability to detect and apprehend suspects, but the celerity with which computer technology is changing and the exponential increase in related criminal activity is broadening the gap. "In FY 1998, the Federal Bureau of Investigation opened 547 computer intrusion cases. In FY 1999, that number more than doubled, with a total of 1154 cases opened. In spite of increases in their ability to close cases, the FBI is realizing a rapidly increasing computer-crime-related caseload. The number of pending cases increased from 206 at the end of FY 1997, to 601 at the end of FY 1998, to 834 at the end of FY 99, and to more than 900 as of March of 2000. These statistics include only computer intrusion cases, and do not account for computer-facilitated crimes such as Internet fraud, child pornography, or e-mail extortion."[2] The U.S. Secret Service and the U.S. Customs Service have realized similar increases in this type of crime.

Additionally, the financial losses being attributed to computer crimes are staggering. The Computer Security Institute released the results of its 6th annual computer crime and security survey on March 12, 2001. Losses reported by 186 of the 538 respondents totaled more than $377 million, an increase of over $100 million from the losses reported by 249 respondents in the 2000 survey. Theft of proprietary information and financial fraud accounted for the largest proportion of loss. The respondents reported across-the-board increases in external system penetrations, denial of service attacks, and virus "infections." Surprisingly, only 36 percent of the respondents reported the intrusions to law enforcement authorities.[3]

Cyber crime poses a daunting challenge to the federal judiciary. While the majority of cases we investigate and supervise are related to the manufacture, distribution, and possession of illicit drugs, case filings involving the use of computers to commit or further a crime are on the increase nationwide.

With rare exception, our system has been slow to embrace technology and is far from able to boast a seat at the cutting edge of technology. We are being asked to supervise and protect the community from a new breed of defendants and offenders (referred to as defendants for the remainder of this article) who not only embrace technology, but also are finding increasingly sophisticated methods to use that technology to further criminal endeavors. We are seeing a phenomenon in

which many traditional crimes are being committed using computers. When this activity takes place across the Internet or through the use of telecommunications, a nexus is present to bring it to federal prosecution and hence into our purview. Another phenomenon of the rapid growth in computer technology and the Internet is that larger numbers of juveniles are entering the system, and being charged with an array of crimes that were traditionally attributed only to adults.[4] The numbers have increased to the extent that legislation was introduced in 2000 seeking to make it easier to prosecute juveniles federally.[5] Other than anecdotal information pointing to escalating numbers of cases being investigated and supervised, we have no organized way to track the totals of computer-related or facilitated crimes in our existing statistical environment. We can only surmise that the number of cases that come under the supervision of the courts closely matches the number of prosecutions initiated by the U.S. Attorney's Office.

Like our law enforcement counterparts, we are not prepared to meet the challenge these defendants pose and must begin to develop methods to effectively supervise and enforce the supervision conditions imposed by the Courts. Only a handful of pretrial services and probation officers throughout the country have the knowledge and experience in technology to even begin to come to terms with some of the issues being raised. Even fewer have recognized this and begun the process of obtaining specific training to facilitate supervising these defendants.

To begin addressing the issues raised by these defendants, we must embark on a developmental process to raise the skill levels of our officers and automation staff to assist us in meeting the challenges supervising persons charged with computer crimes are placing before us. Several areas need to be targeted, including the identification and development of the following:

- Training in investigation methods (including computer forensics and interviewing skills).
- Adoption of the Judicial Conference's Model Search Policy (for those districts that will allow computer-related searches).
- Model wording for computer-related conditions of release.
- Supervision strategies.
- Purchasing computer software tools for tracking and monitoring defendants' activities if they are allowed to use a computer or access the Internet.
- Purchasing specialized hardware to detect and retrieve evidence of violations of release conditions on the defendant's computer.
- Providing training for officers tasked with supervision of these defendants.
- The creation and funding of a forensics laboratory to assist districts with investigations and training.

The course of action the system takes will largely depend on the latitude granted to us by the bench, especially regarding any actions that would fall under the broad umbrella of search authority, which is a supervision tool that traditionally has not been widely used.

Investigation Methods

Investigating "high-tech" defendants should not require the development of a workforce of super computer-literate "Cyber Geeks." What is necessary for officers performing investigations is to acquire a familiarity with the computer-related terminology and to develop a basic understanding of how the defendant is alleged to have used a computer to further or commit the offense. Through training, the officers' awareness will be raised and a level of competency will be established to ensure the integrity of the information we gather. This is very similar to training officers to a level of competence regarding substance abuse issues. Officers do not have to become therapists to effectively gather information, make an accurate assessment of need, and provide the courts with recommendations for responsive conditions to deal with identified problem areas. The Federal Judicial Center took the lead in this education process by developing a Special Needs Offender Series installment on Cyber Crime, which aired on the Federal Judicial Television Network on September 21, 2000.

The most important component of an effective investigation begins with a thorough interview. The insertion of technology into the process does not change the dynamics of effective interviewing techniques. As with any good interview, questioning should lead from general to specific detail and focus on open-ended inquiries. When possible, the officer should attempt to speak with a case agent or the Assistant U.S. Attorney to get information about the charged offense and how computers were involved. Armed with that information, the officer can focus in on pertinent questions to determine areas of risk that may need to be addressed through the imposition of a special condition. The officer should gather as much relevant information from the defendant as possible related to his use of computers, at home, school and/or work. Additionally, information about the type of computer and operating system, as well as what devices may be attached to the computer, who besides the defendant has access to the computer system, and what type of external connectivity the system has, may prove useful to the supervising officer.

These defendants are often very proud of the technology they employ and may tend to give more information than is necessary. It is also possible that they will attempt to befuddle the interviewer with jargon. Having a basic understanding of computers and technology will prepare the officer to deal with this and keep the interview on track. Pretrial services officers need to be wary of steering the questions too closely to offense-specific behavior. Probation officers, on the other hand, may need specific information regarding offense behavior to determine, for example, if guideline enhancements for special skills (U.S.S.G. § 3B1.3) should be applied.

Conditions of Release

The conditions of release for bond, probation, and supervised release are the nuts and bolts of the supervision process. Carefully crafted wording can prove invaluable in assisting the officer in restricting behavior, protecting the community, or providing resources for correctional treatment. Poor wording often leaves room for interpretation, provides defendants opportunities for manipulation, and can be the source of great embarrassment in court settings.

The list of computer-related crimes confronted for investigation and supervision purposes is both varied and constantly changing. The dynamic nature of the law in this area and the continuous advances in technology are making the job of drafting conditions more difficult. In 1999, a working group of probation and pretrial services officers, staff from the Federal Corrections and Supervision Division, and the Federal Judicial Center (FJC) was established to consult with the Federal Judicial Center for the development of their Special Needs Offender Series installment on Cyber Crime. The group's discussions, with guidance from the Office of

General Counsel, led to the development of several items that can be used as guidelines for the development of wording for conditions of release. These were contained in the Special Needs Offender Bulletin, *Introduction to Cyber Crime*, published by the Federal Judicial Center in August of 2000. Another good resource article specific to special conditions for sex offenders by Davis, McShane, and Williams, was published in the June 1995 issue of *Federal Probation*.[6]

We must keep in mind that the number of "new" computer-related offenses (i.e., Denial of Service and Computer Intrusions) being committed by these defendants is relatively small. The majority of cases being filed concern offenses we are very familiar with, but with the added twist that the crime was either perpetrated primarily through the use of a computer or furthered in some way by using computer technology. Examples of these offenses include counterfeiting of monetary instruments and other documents, embezzlement, fraud, drug dealers who store their distribution information or "recipes" on computer media, child pornography, etc. Inasmuch as these offenses are familiar to us, we should be reminded that traditional investigation and supervision methods are still valid. The time-tested conditions of release we have used continue to be legitimate.

When recommending computer-related special conditions of release, the officer should start from the premise that governs decisions for other conditions. Pretrial services officers must determine whether or not the condition 1) addresses a nonappearance issue; 2) addresses an issue of danger to the community or the defendant; and 3) is the least restrictive measure available to assure appearance and negate possible dangerousness. Probation officers recommending conditions should determine if the conditions being considered serve to reduce risk and/or provide correctional treatment. Consideration should also be given to minimizing the amount of intrusion monitoring of the condition will cause in the defendant's life, and reasonably relating the conditions to the offense charged and the defendant. The imposition of a condition prohibiting access to pornography-related web sites may make perfect sense when the offense is related to child pornography or traveling across state lines for the purpose of engaging in sex with a minor. Imposing a similar condition on someone charged with a computer-related fraud would be difficult to justify.

An officer's viewing or monitoring activity and/or logs from a defendant's computer may constitute a type of search. Conditions that allow this activity should not be imposed unless the district has implemented a search policy and is willing to undertake training officers and possibly automation staff to review and retrieve evidence of violations from computers and other digital media. Although we do not have to meet the evidentiary standards imposed on law enforcement agents to prove violations, information collected by officers without authority or in a way that places its authenticity in question may be useless in a violation hearing. This might become especially important if an officer's examination of a computer turned up what appears to be evidence of new criminal activity.

Conducting examinations of a defendant's computer can involve the use of a range of fairly simple software to a combination of sophisticated hardware and software applications. Conditions recommending the use of software tools should be worded based on the experience and ability of the supervision staff conducting the monitoring, as well as the level of computer knowledge and skills the defendant possesses. There are many commercially available programs professing the ability to block access to questionable sites on the Internet that can be easily defeated by persons with minimal computer skills. This is not to imply these "blocking" programs should not be used, but that their limitations should be understood before supervision or accountability problems arise as a result of their use.

Our ability to track or monitor computer use is largely dependent on the presence of information in computer log and history files and system cache directories. There are a number of software programs available that will allow a user to either encrypt or delete this information, thus making it difficult or impossible to retrieve. When recommending special conditions, then, thought must be given to prohibiting the defendant from using software and other technology designed to hide or remove the signs that they have done something to violate their conditions or the law.

A brief outline of computer-specific conditions that could be recommended to the court includes:

- No computer use or access at any location.
- No use of any device capable of accessing the Internet or an online service (i.e., Palm Pilots, Internet Capable Digital Phones, etc.).
- No Internet or Electronic Bulletin Board (BBS) access.
- Provide telephone / Internet service provider billing records monthly.
- Disclose all online accounts, including user-names and passwords.
- No access to modem or other connective device.
- No use of encryption technology or software designed to delete computer log files.
- Require the use of filtering software.
- Use of activity tracking and reporting software.
- Computer search / inspection condition.
- Provide a software/hardware audit at onset of case.
- No new hardware/software added to the computer without officer authorization.

This is by no means a complete list of conditions that could be imposed to address computer-related concerns. Other conditions, including electronic monitoring, third-party risk notification, mental health treatment, and travel restrictions may also be necessary to address identified issues.

Supervision Issues

The increase in case filings at the federal level during the past few years have provided demographic information that is allowing law enforcement agencies to develop a "profile" of defendants. Pretrial services and probation officers across the country report that the three primary groups that are coming into the federal system are: 1) "hackers"; 2) sex offenders who are using the Internet to meet and groom their victims or trade in child pornography; and 3) the traditional criminal defendant who has used computer technology to assist in the commission of a traditional offense such as counterfeiting or fraud.

The demographics suggest that most defendants charged with computer hacking and intrusion-related crimes generally range in age between 15 and 45 years old, are primarily male, and have little or no prior criminal record. They tend to work alone, but like to boast to their peers about their accomplishments (exploits). They are highly motivated and may tend to be manipulative and passive aggressive in authoritative confrontations. Officers supervising defendants in this group need to be mindful that they will tend to try

to obscure information about their personal lives and want to engage in game playing. The officer may be able to take advantage of their love of games and challenges to encourage compliance. These defendants tend to make detailed lists regarding their activities and it would not be uncommon for the lists to be located on the computer or other electronic media.[7]

Defendants being charged with child pornography-related offenses and those charged with traveling across state lines for the purpose of engaging in a sex act with a minor do not fit into a specific demographic profile. The FBI has developed broad classifications for these offenders based on the work of now-retired Special Agent Kenneth Lanning. The classification of offenders most likely to fall under federal supervision is the "Fixated" or "Preferential" sex offender. This classification encompasses individuals who have a specific sexual preference for children and who seek out opportunities to act on their preference. They are highly compulsive, have difficulty forming sexual relationships with age-appropriate peers and often never marry or else enter into relationships of convenience as a cover for their behavior. Their pursuit of victims is carefully planned and they tend to form tight networks within which they trade victim-grooming techniques and trade child pornography.

The second classification is the "Regressed" or "Situational" sex offender. Individuals who fall into this classification may experience a sudden preference for children that coincides with major life stressors including adult relationship or career problems, and alcohol or drug addiction. Members of this group may have a history of relationship problems, and although they become attracted to children, are not necessarily primarily aroused by them.

These defendants, once charged, tend to be mostly cooperative with law enforcement and court-ordered supervision. However, because they are very compulsive in seeking gratification, supervising officers need to remain aware that many will continue to engage in behaviors that may be illegal or dangerous. This increases the risks of home and field supervision. Officers must also keep in mind that these defendants may become suicidal when their behavior is exposed, especially those who have established respectable, usually middle-class "covers" in their daily lives.

These defendants' compulsivity may also work to the advantage of officers monitoring their computer use because they frequently keep diaries of their activities and do not employ sophisticated means to hide their pornography collections. An offender under supervision in the Middle District of Florida is a prime example. The supervising officer received information that the offender might have been engaged in child pornography-connected behavior again. The officer sought and received approval to conduct a search under the district's search policy. During an examination of the offender's computer, the officer located a diary in which the offender had been chronicling his abuse of a number of minor children in the area. Law enforcement was notified and the defendant was eventually charged with a new offense and his release was revoked.

Aside from the specific characteristics of these defendants and the issues arising from their use of technology, officers should find that traditional supervision techniques are effective in gaining and monitoring compliance with conditions. Requiring them to provide documentation of employment, utility billing records, credit card records, and service agreements are a few examples. When practical, enlisting the assistance of family members, employers, and treatment providers will prove invaluable adjuncts to officer supervision.

Computer-Related Searches

Computers can play three distinct roles in a criminal case. A computer can be the target of an offense when the confidentiality, integrity, or availability of its information or services is attacked. Computers can be incidental to an offense when they are used to store drug or fraud transaction data (such as names, dates, and amounts) or to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software). A computer can also be a tool for committing an offense in its capacity as a communications tool. Many of the crimes falling within this category are simply traditional crimes that are committed online. Online facilities may be used to further a broad range of traditional unlawful activity. Email and chat sessions, for example, can be used to plan or coordinate almost any type of unlawful act, including the communication of threats or extortion demands to victims.

In each of these roles, the process involved in creating, saving, and deleting information and files on a computer often leaves information behind on storage media (i.e., hard drives, floppy disks, CD-ROMs) that can be recovered by a trained investigator. In light of this, a new challenge facing pretrial services and probation officers is the potential need to monitor or examine electronically stored information to determine if a defendant has violated the conditions of release.

According to David N. Adair, Jr., Associate General Counsel at the Administrative Office of the U.S. Courts, monitoring the use of a specific computer or connected device through examination of its hardware or software constitutes a "search." The Criminal Law Committee of the Judicial Conference approved a Model Search and Seizure Policy, which was authorized for distribution by the Judicial Conference in 1993, and districts considering implementing search conditions are strongly encouraged to adopt the policy.

The Model Policy is concerned with the methods and conditions under which Probation Officers may conduct searches. Because pretrial services officers have more limited law enforcement authority than probation officers, the Model Policy does not address Pretrial search issues. However, if "*narrowly tailored to fit the needs of a particular individual*," the Court as a condition of release on a bond may specifically grant search authority.[8] The Model Search Policy rightly takes a narrow view of conducting searches and states a search should only be conducted when: 1) there are no alternatives available and 2) reasonable suspicion exists.

Although the location, nature, and volatility of electronically stored information that officers require to verify compliance or document noncompliance with conditions in these cases would appear to warrant periodic random searches, this is strictly discouraged under the Model Search Policy. The Criminal Law Committee stated this type of search should be conducted only when specifically authorized by a special condition of release.[9] Supervising officers should exhaust traditional verification methods, including examination of the records of online service providers (which may require specific release of information or a court order, depending upon the circumstances), billing and credit card records, as well as service contracts, before resorting to a search. Districts considering recommending the imposition of search conditions should first develop and adopt a search policy.

Once issues related to establishing a search policy are dealt with, consideration has to be shifted to the technical aspects of conducting

a search on a computer. If the defendant has been prohibited from possessing a computer or some type of telecommunications device, service, or program, a physical "plain view" search of the home may be the only method necessary to verify compliance. If the court allows the defendant to use a computer or have access to the Internet, it may become necessary to employ more sophisticated monitoring techniques, including a "physical" search of the computer. This step should not be embarked upon lightly, nor should it be initiated without specialized training. If proper precautions are not taken, the data stored on the computer, data disks, or any number of other peripheral devices can be altered, destroyed or rendered inadmissible for court purposes. There is currently no case law spelling out when computer searches by a probation or pretrial services officer are permissible and what the limitations of such searches are.[10]

Depending on the skill level of the defendant, data could be stored in hidden sections of a hard drive, renamed to look like an innocent file type, encrypted, password protected, or may have been deleted. Special tools and skills are required to locate and attempt to retrieve data that has been altered in these ways. In spite of how fast computers operate, conducting a thorough inspection and retrieving documentation of condition violations or new law violations can be a very time-consuming operation, so staff resources must also be a concern.

Consideration must also be given to the level of involvement of automation personnel in the process. There have been instances in several districts where automation staff members have been asked to accompany probation or pretrial services officers to assist with a search or retrieval of information from a computer system. Thorough examination of such a practice may lead to the conclusion that it ought not be allowed to continue. The search of a home, or a computer in a defendant's home, should be considered a potentially volatile and dangerous undertaking. Automation personnel have neither the training to protect themselves and others in a dangerous situation nor do they enjoy benefits of the hazardous duty designation shared by probation and pretrial services officers. A more prudent approach might involve training officers in the specific skills needed to retrieve an exact copy of the data on a computer and returning it to the automation staff or a trained officer to conduct a thorough forensic examination of the data.

The issue of searching and seizing data from computers also raises concerns about privacy, not only of the defendant, but also of third parties who may reside at the same location and share access to computers. The Electronic Communications Privacy Act (ECPA -18 USC §§ 2510 & 18 USC §§ 2701)[11] impacts information and data that may be housed on a computer system. An examination of the statutes indicates that in dealing strictly with the search of a defendant's computer, pretrial and probation officers probably do not have to be concerned about exposure to civil or criminal penalties, except when dealing with unopened email. Depending on the physical location of the message (whether it is on the defendant's computer or a remote server), ECPA provisions may proscribe the viewing of the unopened message.

If the defendant shares the use of a computer with one or more parties, it could be possible to violate the act and be subject to sanctions. Methods to address this issue may include use of written consent forms and posting of a notice on the computer that its contents are subject to inspection. For defendants released on a bond, there is also the possibility of making the persons who share access to the system custodians on the bond, thus giving them a vested interest in ensuring compliance with the conditions.

The impact of technology and the rise in computer-related crimes may cause the field to seek additional guidance regarding computer searches from the Judicial Conference. In the meantime, it appears that the best course of action would be to pair the implementation of a search policy with special conditions of release to allow for random searches limited to address specific behavioral controls such as enforcing a prohibition against possession of pornographic material or use of encryption technology.

Training Issues

A handful of districts in the country have begun to research and use methods to monitor defendants' computer use and to conduct computer examinations to corroborate compliance problems. Most have entered into this technological quagmire with little or no expertise other than an officer who had a keen interest in technology and a willingness to experiment. Through the efforts of the Federal Judicial Center and the Federal Probation and Pretrial Services Officer's Association, awareness is being raised and it is being recognized that in order to preserve the integrity of the information we provide to the court, we must become appropriately trained in forensic techniques.

Fortunately, several federally funded agencies have opened the doors to allow probation and pretrial services officers to attend forensics training. Among these is the National White Collar Crime Center (NW3C), the Federal Law Enforcement Training Center (FLETC) and SEARCH, The National Consortium for Justice Information and Statistics. While initially reluctant to provide training to non-traditional law enforcement officers, these organizations have since recognized the efficacy of providing training to our field. This shift was, in part, due to the growing backlog of examinations being experienced by computer forensics labs operated by the Federal Bureau of Investigation, the U.S. Secret Service, and U.S. Customs Service.

These programs offer basic and advanced computer forensic training courses and cover topics from identification of computer hardware to examining and retrieving digital information from hard disks and other digital media. The programs provide an assortment of free tools to assist in the examination process and expose attendees to several commercially available applications designed to streamline the information recovery process. Districts considering adopting a search policy and embarking on monitoring of defendants' computer use should consider making the training available. Officers who wish to attend one of the basic courses should possess a working knowledge of computers and the MSDOS and Windows operating systems at a minimum. Completion of a basic forensics course is usually a prerequisite for participating in an advanced program. Demand to participate in the programs is high and there are waiting lists to attend. The classes last from one to two weeks and tuition costs range from free to several thousand dollars.

Establishing a Forensics Laboratory

While staff training is being completed, consideration should be given to setting up and equipping a laboratory to facilitate the analysis process. In some cases, attempting to conduct an analysis in the field is not practical, nor is it the safest method to employ. The ideal, according to forensic investigators from the FBI and U.S. Secret Service, is to obtain an exact copy or image of the media to be examined in a secure laboratory setting fol-

lowing the seizure of the suspect computer. In some instances, when seizure is not possible, this image may be obtained in the field and then removed to the laboratory. For probation and pretrial services purposes, seizure may not be the least intrusive method to utilize, but cannot be ruled out if an image cannot be obtained safely or in a timely fashion.

An assortment of hardware and software is necessary to establish a viable lab. The exact configuration depends on a number of factors, including the training level and abilities of the examiner. Access to a number of computer operating systems, including MSDOS, Windows (Version 3x through 2000 and Windows NT), and Linux/Unix is necessary. Laboratory workstations need to be flexible enough to allow the examiner to easily add and remove hardware and be robust enough to perform memory-intensive search and retrieval operations. The lab should be equipped with a variety of external storage devices (i.e., SCSI and IDE CD-ROM and Hard Disk Drives, Iomega Zip and Jazz Drives) or have a budget flexible enough to allow for the purchase of additional devices as may be necessary.

In addition to the laboratory workstations, a portable workstation is recommended to allow for a less intrusive "preview" of a system using software tools to look for specific file types or information. If no violations are evident, it may not be necessary to take further action. The portable unit would facilitate field examinations of a computer system if absolutely necessary, and would allow the examiner to perform analyses at remote locations such as a remote division office. Any portable system should be configured with a variety of storage device options to allow for the retrieval of disk images in as short a time as possible. While smaller and portable, the unit should be able to perform the same software tasks as a laboratory workstation. Some examiners choose to use laptop systems with external storage device options, while others profess that a "luggable" type system that is a scaled-down version of a desktop computer with removable drive bays and an attached LCD monitor is the best option for a portable field workstation.

There are few companies producing forensically sound integrated software to perform an examination on a computer. Unfortunately, the market is still small, so the software tends to be expensive and often requires the examiner to receive additional training to gain a level of proficiency with it. There are a number of sources for "free" applications and utilities that perform some of the tasks that are automated by the integrated applications, but they also carry a steep learning curve and, because they are not integrated, tend to require more time to perform the same functions as the integrated packages. Information disseminated in the training programs sponsored by the NW3C and FLETC as well as discussion with active forensic examiners indicates that the favored procedures are to use an integrated package to perform the analysis on a system and then use the standalone applications to corroborate findings. In addition to the actual forensic software packages, many labs use commercially available programs to recover or "crack" password protection schemes built into popular word processing, spreadsheet, and database applications.

The costs of establishing a functional forensics examination lab are another concern. The Bexar County District Attorney's Office in San Antonio, Texas, recently received a grant to fund the establishment of a computer forensics laboratory. They initially budgeted $16,000 for equipment and $11,000 for software. They purchased three standalone workstations for the laboratory, a "luggable" system to perform field analysis, two portable hard-drive duplicating devices, as well as an assortment of software and remained within their budgetary constraints. These costs are not out of the ordinary for a small laboratory, according to members of the Computer Forensics Information Digest (CFID), an Internet-based discussion group comprised primarily of forensic investigators at the federal, state, and local level. Any budget for the establishment of a lab should also include allowances to purchase new technology, larger form-factor storage devices as they become available, software updates, and ongoing training for the examiners.

The cost of establishing a laboratory, when coupled with the expenses related to staff training, may be prohibitive for many districts. A subgroup of probation and pretrial services officers who were involved with the FJC on the Special Needs Offender program on Cyber Crime formulated a proposal for the establishment of one or more regional laboratories to serve as a resource for forensic analysis and training. With the support of both a Chief Pretrial Services and Chief Probation Officer, the proposal has been submitted to the Federal Corrections and Supervision Division of the Administrative Office of the U.S. Courts and steps are being taken to analyze the proposal.

Conclusion and Recommendations

The explosive growth of the Internet and concomitant advances in technology during the past decade have spawned a new breed of criminal and provided a plethora of tools to aid more traditional criminals in their endeavors. Regrettably for those of us in the criminal justice system, the "bad guys" gained an early advantage. The knowledge vacuum created in our system by their nimble adoption of technology has been recognized and is being addressed as rapidly as possible. Training programs for law enforcement agencies have shifted into high gear in an effort to close the knowledge gap. Unfortunately, the growth in new case filings is currently outdistancing the ability to train investigators and is resulting in growing backlogs of investigations and prosecutions.

Congress has recognized the threat posed by computer crime and is in a mode similar to when they began enacting legislation to deal with the looming menace of "crack" cocaine. New laws are being introduced to address new crimes and enhance penalties on old crimes that are being committed using computer technologies. Commissions have been formed to address the problem within our borders and internationally. Since 1992, the U.S. Department of Justice has asked the U.S. Sentencing Commission to promulgate new guidelines and enhance others to ensure that offenders convicted of high-tech crimes are appropriately sentenced.

Where does this leave the courts? Across the country, U.S. pretrial services and probation officers are reporting increases in number of cases coming to them for investigation and supervision. Since specific computer-crime statistics are not tracked, only anecdotal information can be used to advise the Judicial Conference and the Administrative Office and/or to request guidance and assistance. Just looking at the growing numbers of cases under investigation and pending prosecutions should be enough to warn of an impending crisis. Instead of waiting until another congressionally targeted initiative like the "Weed and Seed" program from the mid-1990s is at our doorstep, or until the knowledge gap among the law enforcement agencies begins narrowing, the courts must take a proactive stance.

This suggests the initiation of a campaign to meet the challenges posed by these technologically savvy defendants. A four-tiered line of attack that incorporates the strategies outlined above includes: 1) the identification or

hiring of qualified staff; 2) the development of training programs (both internal and external); 3) the adoption of computer search/seizure policies; and 4) the creation and funding of one or more regional laboratories to conduct forensic examinations.

The foundation for this initiative has already been laid. Resources have been identified and a growing pool of expertise is available within the probation and pretrial services system to tap for assistance. This is the proper time for the Federal Corrections and Supervision Division to take the lead in establishing a program, with assistance from the field, for presentation to the Criminal Law Committee and eventual adoption by the Judicial Conference.

References

1. Children Families and the Internet 2000, a survey of 1,735 parents of children aged 2-17, and 601 children aged 9-17 from the same households. Grunwald Associates, 1793 Escalante Way, Burlingame, CA 94010. (**www. grunwald. com**)

2. From the Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information,Washington, D.C. March 28, 2000. **http://www.cybercrime.gov/freeh328.htm**.

3. "Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey," Computer Security Institute. **http://www.gocsi.com.**

4. Arthur L. Bowker, "The Advent of the Computer Delinquent," FBI Law Enforcement Bulletin, Volume 69, No. 12 (December 2000): 7-11.

5. Internet Integrity and Critical Infrastructure Protection Act of 2000. The bill, introduced by Judiciary Committee Chairman Orrin Hatch of Utah, lost some of its strictest measures in the debate process, as some argued that its original guidelines would over-federalize many minor offenses. For example, the bill originally would have authorized federal prosecution of any juvenile accused of a felony computer crime. As amended, the bill calls for federal prosecution of juveniles only for the most serious offenses.

6. Laura Davis, Marilyn D. McShane, and Frank P. Williams, III, "Controlling Computer Access to Pornography: Special Conditions for Sex Offenders," *Federal Probation* June 1995.

7. Ed Harrison, "Supervising the High-Tech Offender," 1998.

8. Letter from David N. Adair, Jr. Associate General Counsel, to Mr. Joseph P. Brignone, U.S. Probation Officer, Buffalo, NY, dated March 17, 1998.

9. Mark Sherman, "Issues and Tools for Investigation and Supervision," *Special Needs Offenders Bulletin: Introduction to Cyber Crime*, August 2000.

10. David N. Adair, Jr., Associate General Counsel, "Guidance on Searches and Seizures," *News and Views*, Vol. XXVI, No.8 (April 9, 2001).

11. ECPA updated title III, Omnibus Crime Control and Safe Streets Act of 1968. It extends privacy protection to modern technologies and primarily impacts the wiretap statute (18 USC §§ 2510 - http://www4.law.cornell.edu/uscode/18/ch119.html#PC119) and stored communications access statute (18 USC §§ 2701 - http://www4.law.cornell.edu/uscode/18/ch121.html#PC121). It was primarily designed to protect *contents* of electronic mail, voice mail, and remote computing services.

Computer Crime in the 21st Century and Its Effect on the Probation Officer

Arthur L. Bowker, U.S. Probation Officer, Northern District of Ohio
Gregory B. Thompson, U.S. Probation Officer, Southern District of Indiana

IN TODAY'S TECHNOLOGICAL environment, the computer is becoming not only a beneficial aid for law enforcement, but the tool of choice for a new generation of offenders. Computers are now used to facilitate many traditional crimes, as well as new "cyber crimes." Two years ago, the typical computer offender was an employee taking advantage of an employer's computer system. More recently, "hackers" have manipulated the computer systems of the White House and the FBI, agencies whose security measures are among the best. As the 21st century commences, hacking and other computer offenses will become increasingly common. This requires law enforcement agencies and probation offices to be staffed with computer-literate employees. This article specifically addresses what probation offices can do to assist the courts in effectively supervising the computer offender. We also will suggest investigative techniques and possible special conditions for computer offenders. Finally, we will mention what steps the U.S. Sentencing Commission has taken in writing guidelines for computer offenders. As more computer criminals enter the probation offices across the country, it is evident that computer knowledge will be necessary. Probation officers must become computer savvy to keep up with the ever-changing offender.

Consider the following:

- A 30-year-old compulsive gambler, convicted of embezzlement, is placed on six months home confinement with electronic monitoring at his parents' home. This offender begins "surfing the net" on his father's computer and quickly locates numerous gambling sites. Unbeknownst to his parents or his supervision officer, he begins gambling in "cyber-space," which is a clear violation of a no-gambling condition imposed by the court.
- A 54-year-old male, convicted of receiving child pornography through the mail, secures employment at a large corporation. Although his computer experience is limited, he is allowed Internet access. Within a few weeks he begins "exploring" adult entertainment sites until he finally downloads child pornography.
- A probation officer is assigned a presentence investigation report on a defendant who "hacked" into a local airport's computer system. During the home visit, the probation officer notes an extensive computer system. What conditions can the probation officer recommend to the court? Do those recommendations change if the defendant relies heavily on that system in his employment?

To address computer offenders, probation officers need to develop unique investigative and supervision techniques to improve their ability to complete presentence investigation reports and recommend and enforce conditions, risk control, correctional treatment, and community protection.

Investigations

Although computers are a new instrument, probation officers need not discard their traditional investigative techniques. Traditional techniques, such as interviewing collateral contacts and examining records, are extremely important means of identifying problem areas. We believe such traditional techniques should be considered first before jumping into more technical and problematic areas of investigation. Interviews with third parties and the offender may reveal how the computer was misused during the offense or evidence that a computer or the Internet is being misused during supervision. Employer contacts can reveal that the offender has access to the Internet, or that a third-party risk exists. Interviews with family members and significant others can provide information on where, when, and for how long an offender is using the Internet. For instance, an interview with the mother of an offender who is prohibited access to the Internet may disclose that he began spending an enormous amount of time at the local library. A subsequent interview with the librarian may disclose that the offender has been admonished several times for exceeding the allotted time on the library's Internet computer. Moreover, knowing the time frame of use can narrow the scope of a computer system search when such a technical step becomes necessary.

Various forms of record examination can also be beneficial. Reviewing "hard copy" documents such as bills, telephone records, and computer printouts may reveal signs of computer usage or Internet access. Telephone bills may reflect billings for multiple lines into the offender's home, one of which may be used for a computer. A credit check, or credit card and bank statements may reflect Internet access charges, on-line debits/credits (indicative of Internet gambling), or large purchases at office supply or computer stores. Other records the officer can examine are sign-in

sheets or similar logs that may be maintained by employers, local libraries, or universities to record computer/Internet usage.

All officers should be aware that any documents provided by an offender are subject to computer manipulation and/or falsification. Probation officers should always look for possible inconsistencies over time in the documents provided by an offender. These inconsistencies may be signs that the documents are bogus. For instance, an offender, reportedly working for a sales company that employs over one hundred people, provides monthly pay stubs numbered 100, 115, and 110. It is highly improbable for a company of a hundred or more employees to have paid this offender with checks that are only a few digits off from one another over a six-week period. As is always the case, third-parties should be contacted to verify any information provided by an offender.

With the advent of technology, not only have the offenders been advancing, but so have the law enforcement professionals. For example, a number of software programs are available to monitor the computer activity of an offender. Examples of districts using computer monitoring and filtering programs to supervise certain computer offenders are the Southern District of Indiana, Middle District of Florida, the Southern District of New York, Western District of Texas, and the Western District of Wisconsin. Monitoring programs are designed to capture the sites an offender visits by either recording the sites visited and/or sending a screen snapshot every time the offender is on line. Filtering programs prohibit the offender's access to certain web sites. Some critics believe these software packages are too new to the probation field and need refining. One chief concern is that such programs can provide a huge influx of information needing to be reviewed on a regular basis, thus overloading the probation officer. Filtering software, on the other hand, has been criticized for not blocking what it is intended to block, as well as blocking sites it shouldn't. Additionally, there are numerous hacker sites that provide detailed information on how to overcome filtering software. Youths have been known to access these sites to circumvent parental controls. Such software programs are beneficial, but at this juncture they tend to be more advantageous for the less sophisticated user. The more knowledgeable the offender, the more likely he is to manipulate the program to his liking. As probation offices work with the software manufacturers, this may change (Collette, 2000).

Monitoring/filtering software should be considered as one supervision tool, but not the only one at the probation officer's disposal. A limited computer search should be used to insure the software has not been compromised by the offender. Additionally, the software or other sources of information may establish a "reasonable suspicion" that the offender has violated a supervision condition. The results of the monitoring software can then be used as a basis for a more intrusive computer search and/or seizure.

Supervision of Computer Offenders

Although the best condition for any computer offender may be no computer at all, there are three areas of concern regarding such a broad restriction. First, some argue that the term "computer" is becoming an increasingly difficult word to define. If a condition ordered states "the offender is to refrain from having access to a computer while on probation, unless authorized by the probation officer," the definition of computer is too general. Is a computer the CPU, the monitor, the scanner, the software, the keyboard, or is it also a pager, a cell phone, and a palm pilot organizer? Technology is advancing in that cell phones, pagers, and organizers have access to the Internet. What is allowed and what is not allowed?

Fortunately, there is some guidance on this first issue. Painter (2001) notes that Kevin Mitnick, a notorious hacker, argued before the District and Appellate Courts ". . . that broad conditions restricting access to computers are fatally vague and overboard." His argument was that computer chips are in everything from automobiles to toasters and that he would be forced to live like a hermit or commit unintentional violations of his supervised release. Both courts rejected this argument, noting conditions restricting computer access should be read in a commonsense manner. Painter cites the following court case to support this interpretation:

> [F]air warning is not to be confused with the fullest or most pertinacious, warning imaginable. Conditions of probation do not have to be case in letters six feet high, or to describe every possible permutation, or spell out every last self-evident detail [they] may afford fair warning even if not precise to the point of pedantry. In short, conditions of probation can be written-and must be read in a common sense way. *United States v. Gallo*, 20 F.3d7, 11 (1st Cir. 1994). (internal citations omitted) (p. 48)

The second concern with a no-computer condition is that computers are becoming a more integral part of everyone's lives. In one form or another, they are now found in every work and educational environment in the nation. Consequently, judges may not wish to prohibit all access to computers, so specific conditions regarding the Internet, bulletin board systems (BBS), and chat rooms may be more appropriate.

Finally, the no-computer condition typically includes the phrase "unless authorized by the probation officer." Such wording provides the probation officer the authority to either completely restrict or give authorization in certain circumstances. Absent appropriate training and/or court guidance, some probation officers may be inclined to simply deny any access without regard to the particular circumstances of a case. Such blanket denials may not always pass court scrutiny. Again, Kevin Mitnick tested his supervision officer's resolve. One of Mitnick's conditions directed that he was ". . . not [to] act as a consultant or advisor to individuals or groups engaged in any computer activity, as directed by the probation officer." In part because of his notoriety, many of Mitnick's employment offers involved computers. Mitnick did not first present the details of these offers to his probation officer for a decision. Instead he chose to proceed directly to the court, arguing that his probation officer had denied him the opportunity to work. The District Court concluded that blanket decisions were unacceptable without consideration of the specific offers. Since this decision, the probation officer reviewed the employment offers and Mitnick now writes, consults, and speaks on computer-related subjects. This is a prime example of a highly intelligent offender questioning the discretionary decision of the probation officer. When computers are essential to an offender's livelihood, it is likely that courts will follow what has occurred in the Mitnick case. Therefore, probation officers need to know how to supervise an offender who is allowed limited access to computers, or is allowed to be employed as a consultant to computer companies (AP, 2000).

To address these changing times and to avoid later difficulties, a probation officer must be qualified to conduct an educated assessment of a computer offender before he/she makes a recommendation for special conditions. Additionally, courts in the future may ask the probation officer what type of special conditions should be ordered in "high-tech"

cases. To answer such questions, we must be prepared to make an accurate and exhaustive assessment. Assessment entails obtaining and evaluating information about the offender and the offense to address a computer risk. Any assessment of computer risk must examine the conviction offense, the computer knowledge and ability of the offender, prior criminal conduct involving computers, the necessity of the offender having computer access, and the availability of a computer or the Internet. An accurate assessment of these factors will ensure that special conditions regarding access to a computer are in congruence with 18 U.S.C. §§ 3553, 3563, and 3583.

In the Mitnick case the Central District of California imposed some of the most restrictive computer conditions imaginable. However, these conditions were necessary in view of Mitnick's repeated history of committing high tech crimes. Mitnick had previously been on supervised release for a computer offense. He absconded from that supervision and became a fugitive committing additional computer offenses. Painter notes:

> In imposing the extensive conditions of supervised release, the judge held a number of hearings and based her ruling on defendant's long history of hacking, defendant's inability to comply with less onerous restrictions and, most importantly, the need to protect the public. The court's focus on the "tools" Mitnick has habitually used to commit past criminal conduct, computer and cellular phones, was wholly appropriate given defendant's seeming inability to use these tools in a law-abiding manner. Given his past extensive and repeated criminal conduct, and the prospect that, unsupervised, he would be tempted to engage in the conduct again, the court expressly stated that the conditions were designed to protect the community. . . . (pp. 45-46)

Table 1 provides some suggested computer conditions based upon the degree of computer/Internet access that is appropriate to a particular case.

A lack of special conditions regarding computer crime does not authorize the probation officer to neglect the offender's access to computers. As previously stated, computers are used to further many crimes outside of fraud and child pornography. Therefore, the probation officer still has many investigatory areas to develop in risk control and prevention. Simple techniques such as browsing a history icon or bookmarks can reveal evidence of violations for the less sophisticated offender.

More intelligent offenders may require more advanced techniques. They may also require more advanced conditions or special orders from the court. Most courts will not issue such an order without substantial evidence. We believe advanced forensic techniques are better left to those who have received the appropriate training in computer investigations and forensics. With the appropriate authority, the ability to search an offender's hard drive and locate hidden or erased files can provide valuable information on an offender's activities. Knowing how to download selective files and make a "logical copy" and a "mirror image" of a hard drive for later in-depth examination also facilitates the detection of illegal activity (See Table 2). More intrusive methods involve seizing the offender's computer for forensic examination by others.

Examining media storage devices (i.e., disks, hard drives, zip drives, tapes, etc.) is a very time-consuming task. Many of these devices can now store millions and millions of bytes of information. For instance, 1 gigabyte (GB), currently a small size in data storage, holds 1,073,741,824 bytes of information or the equivalent of a pickup truck filled with paper. Suggested time frames for searching a 3 GB hard driver are as follows: 3 kilobytes (KB) equals one page; 3 GB equals 1,000,000 pages. Time to review: 5 seconds/page, 12 pages/minute, 730 pages/hour, 17,280/day, total review 58 days. These time frames do not assume keyword searches or other techniques for narrowing the search (Bowker, 2001). Probation officers would be well advised to use traditional investigative techniques to limit the scope of their examinations as previously indicated.

Moreover, gaining access to an offender's computer at the workplace also presents difficulties for the probation officer. A work-site computer may be connected to a mainframe, a local area network (LAN), or a wide area network (WAN). In addition, there are obvious liability concerns for accessing a work-site computer, such as inadvertent damage to system. Because of these intricacies, gaining permission from the employer is a legal requirement.

Seizing a computer takes very specific skills and knowledge. Evidence can be lost by merely turning on the system without the proper procedures in place. The offender may also have "hot or test keys" that when struck activate programs that either destroy or encode data. There can also be civil and criminal penalties for improperly seizing a computer. These are just a few examples of things that might go wrong for someone who has little expertise in computer seizure procedures. *The Model Search and Seizure Guidelines* (Judicial Conference of the United States, March 1993) also discourages search and seizures. This policy statement, coupled with the technological complexities of computer evidence, make seizing a computer a last resort for a probation officer.

Use of the Computer by the Probation Officer

Although computers can facilitate crime, they can also assist officers in the investigative process. For instance, the Internet is a vast collection of information that is stored in hundreds of thousands of connected computers throughout the world. The Administrative Office of the United States Courts (AO) noted the following in its publication, *Internet Resources for Probation and Pretrial Services Officers* (1998):

> Probation and Pretrial Services Officers are called upon to collect personal data on individuals who are under bond consideration, pending sentencing, or under supervision. National telephone directories, street maps, and address locators are available on the Internet with easy to use graphical computer screens. Financial and social histories of individuals can be developed through on-line periodical searches. Current information (e.g. publications, articles, scholarly works) on substance abuse detection and treatment, mental health, and criminal justice are readily available.(p.2)

Cadigan (1998) noted several innovative uses of the Internet by probation officers. Specifically, probation officers have used the Internet to obtain information regarding street and prison gangs, militia groups, and "hate groups." Other officers have used the Internet to obtain information on the newest suggested techniques for defeating drug testing. One officer used the Internet to detect web pages developed by a sex offender with a special condition prohibiting him from using the Internet.

Siuru (1999) also reports the Internet is now being used by various courts to directly obtain information. Siuru indicates that G.T.E. Corporation has developed "The Bastille," an "Internet-based information-sharing service for law enforcement." The Bastille will permit the secure exchange of information between various law enforcement subscribers. Cadigan correctly predicts

TABLE 1
Suggested Computer Conditions

(A=Internet Access Permitted, B= Limited or No Access to Internet)	A	B
You shall consent to your probation officer and/or probation service representative conducting periodic unannounced examinations of your computer(s) equipment which may include retrieval and copying of all memory from hardware/software to ensure compliance with this condition and/or removal of such equipment for the purpose of conducting a more thorough inspection; and consent at the direction of your probation officer to having installed on your computer(s), at your expense, any hardware or software systems to monitor your computer use or prevent access to particular materials. You hereby consent to the periodic inspection of any such installed hardware or software to insure it is functioning properly.	X	X
You shall not possess encryption or steganography software.	X	X
You shall provide your probation officer accurate information about your entire computer system and software; all passwords used by you; and your Internet Service Provider(s).	X	X
You shall possess only computer hardware or software approved by your probation officer. You shall obtain written permission from your probation officer prior to obtaining any additional computer hardware or software or Internet Service Provider(s).	X	X
You shall refrain from using a computer in any manner that relates to the activity in which you were engaged in committing the instant offense or violation behavior, namely _____.	X	X
You shall provide truthful information concerning your identity in all Internet or E-Mail communications and not visit any "chat rooms" or similar Internet locations/sites where minors are known to frequent.	X	
You shall maintain a daily log of all addresses you access via any personal computer (or other computer used by you), other than for authorized employment, and make this log available to your probation officer.	X	
You shall not create or assist directly or indirectly in the creation of any electronic bulletin board, Internet Service Provider, or any other public or private network without the prior written consent of your probation officer. Any approval shall be subject to any conditions set by the U.S. Probation Office or the Court with respect to that approval.	X	X
You shall not possess or use a computer with access to any "on-line" computer service at any location (including employment or education) without prior written approval of the U.S. Probation Office or the Court. This includes any Internet Service Provider, bulletin board system, or any other public or private computer network. Any approval shall be subject to any conditions set by the U.S. Probation Office or the Court with respect to that approval.		X
You shall not purchase, possess, or receive a personal computer which utilizes a modem, and/or an external modem.		X
You will have an occupational condition that you can not be employed directly or indirectly where you are an installer, programmer, or "trouble shooter" for computer equipment.	X	X

TABLE 2
Basic Computer Retrieval Techniques

Downloading	Process of copying selected computer files. Process does not take much time.
Logical Copy	Copies all non-hidden files and non-hidden directories. Moderate amount of time involved, depending upon number of files/directories.
Mirror or Duplicate Image	Is an exact copy of everything, including hidden files/directories, data remaining from erased files/ directories. Also includes information from unused space. Moderate amount to extreme amount of time, depending upon the media being duplicated. Not unusual for new disk drives to take 12 or more hours, depending upon equipment used.

"as officers become more familiar with information that can be accessed through the Internet, it will play an increasing role in enhancing work practices and help officers 'work smarter, not harder.'"

Stored Wire and Electronic Communication

Probation officers must understand the statutes pertaining to e-mail and other forms of stored electronic communication. Federal law, specifically 18 U.S.C. §§ 2701-2771, provides for both criminal and civil penalties for anyone who accesses without or in excess of authorization a facility through which electronic communication services are provided, " . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while in electronic storage." Probation officers supervising offenders must not access any unopened e-mail or similar electronic communication in storage without specific authorization of the court or consent of the offender. E-mail that has been opened and saved to an offender's system is not covered by this provision. Some offenders may be providing e-mail services on their computer systems to other individuals. Under no circumstances should a probation officer access any e-mail or similar electronic communication in storage pertaining to other individuals without appropriate legal consultation and approval of the court.

Privacy Protection Act

Any offender with a computer, particularly one with a modem, can be considered a publisher within the meaning of the Privacy Protection Act (PPA), 42 U.S.C. § 2000AA. The PPA provides for civil penalties for anyone who seizes, without a subpoena, work products or documents that are intended for dissemination to the public. Work products or documents can be saved electronically in a computer. The following are general exceptions to this provision: information that is contraband or fruits of instrumentalities of the crime (i.e., child pornography, illegally copied software); information that is evidence of crime committed by the subject (i.e., diary confession to a particular offense); to prevent death or serious injury; subpoena has been tried and failed; or reason to believe that a subpoena would result in destruction of evidence. In *Steve Jackson Games, Inc. v. U.S. Secret Service* (1993), agents were found to have violated the PPA when they failed to return computers after it was learned they contained PPA-protected material. The plaintiff was awarded over $300,000 in damages, attorney's fees, and costs. As always, probation officers should obtain legal consultation when dealing with the PPA or stored electronic communications.

U.S. Sentencing Guidelines

In June of 1996, the U.S. Sentencing Commission reported to Congress on two broad areas involving computer use by offenders. The first dealt exclusively with violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). This study found that approximately 60 individuals had been convicted of this statute. Their profile of the "typical offender" was noted as follows:

> . . . computer criminals tend to be somewhat better educated individuals who have less significant criminal histories than those convicted of other federal crimes...the typical computer criminal has not been a sophisticated user, but is, rather, likely someone with a pedestrian level of computer expertise who misuses his employer's computer system in committing his offense. (U.S. Sentencing Commission, Adequacy of Federal Sentencing Guidelines, p. 8)

This study concluded that no definitive assessment could be made on the deterrent effect of the existing guidelines on computer crime because of:

> . . . 1) an inability to determine how much computer crime was occurring before the guidelines went into effect, 2) the relatively small number (approximately 60) of the guideline convictions to date under the pertinent statute, and 3) the general difficulty of determining the deterrent effect of any criminal sanction. (U.S. Sentencing Commission, Adequacy of Federal Sentencing Guidelines, p. 8)

At the time, the Commission was consulting with the U.S. Department of Justice's Computer Crime Division on proposals to amend the guidelines to account for anticipated increases in computer crime. Note that the U.S. Sentencing Commission's findings were based *solely* upon cases of individuals convicted of violating 18 U.S.C. § 1030. We strongly suspect a great deal of computer offenders may be lost in such tracking devices because computer crimes may be prosecuted under other statutes. This is possible because the statutory maximum penalty for 18 U.S.C. § 1030 is typically five years (It can reach 10 and 20 years, but only if the computer data was restricted due to reasons of national defense or foreign relations.). Offenses involving computers are frequently prosecuted under other statutes carrying stiffer penalties. One example is 18 U.S.C. § 1344, bank fraud, which carries a 30-year maximum term of imprisonment.

The report further noted computer use is evolving rapidly. For example, although the overall numbers remained small, computer use in federal child pornography cases grew by 5 percent between 1994 and 1995. In response to congressional mandates, the Sentencing Commission also amended the guidelines to provide for a two-level upward adjustment for cases of child pornography involving computer use (See U.S.S.G. § 2G2.1 (b) (3), U.S.S.G. § 2G2.2 (b) (5), U.S.S.G. § 2G2.4 (b) (3)). (SOAC, p. 30).

Just four years later, in May, 2000, the U.S. Sentencing Commission sent new guidelines to Congress proposing much stiffer penalties for "high-tech" crimes. These guidelines have since taken effect. In some cases, the specific guidelines more than doubled the sentence for computer and other high-tech crimes. For example, an offender who used the Internet to meet minors and engage in sexual relations had a potential guideline range of 18 to 24 months increased to 41 to 51 months. Other guideline changes covered offenders who steal the identities of credit card users and make them available on the Web for widespread use. These guidelines increase the penalties from typically probation, to a prison term of 15 to 21 months. An increase in the guideline range for violations of copyright or trademarks online was also adopted. (United States Sentencing Commission, *Guideline Manual*, November 1, 2000, United States Sentencing Commission, *Supplement to the 2000 Guidelines Manual*; Brunker, 2000; and Fields, 2000.)

There is also some precedent for the application of the guidelines in computer crime cases. In *U.S. v. Petersen* (1998), 9th Circuit, an enhancement for special skill pursuant to U.S.S.G. § 3B1.3 was warranted for a computer "hacker," who hacked into several sites and manipulated the phone lines of a radio station to win a car being awarded by the station. The Appeals Court found that the lower court did not err in assessing the special skill enhancement, pursuant to §3B1.3. However, in *U.S. v. Godman* (2000), the 6th Circuit Appeals Court recognized that a special skill enhancement was not appropriate for a defendant who had no formal computer training and had used desktop publishing software from a local retailer to counterfeit

currency. The Appeals Court in this case concluded:

> At a time when basic computer abilities are so pervasive through society, applying §3B1.3 to an amateurish effort such as Godman's would threaten to enhance sentences for many crimes involving common and ordinary computer skills. The Guidelines contemplate a more discriminating approach. (p.3)

Additionally, recent changes to the Guidelines reflect that an enhancement under §3B1.3 is warranted for a defendant who de-encrypts or otherwise circumvents a technological security measure to commit a criminal infringement violation (United States Sentencing Commission, *Supplement to the 2000 Guidelines Manual*, p.54).

In *U.S. v. Hibbler* (1998), 6th Circuit, a five-level increase for distribution of child pornography was warranted for someone who traded child pornography on the Internet, even though they received no "pecuniary gain." In *U.S. v. Williams* (1992),10th Circuit, an enhancement for "more than minimal planning" was appropriate for an embezzlement occurring over six months and involving numerous computer entries.

Other case law exists on the appeal of special conditions by a defendant. In *U.S. v. Crandon*, (1999) 3rd Circuit, the district court ordered the following condition: "The defendant shall not possess, procure, purchase, or otherwise obtain access to any form of computer network, bulletin board, Internet, or exchange format involving computers unless specifically approved by the U.S. Probation Office." The defendant lured a 14-year-girl via the Internet to a remote location, engaged in sexual activity, and also took photos of the young girl. The appeals court upheld the condition, stating the lower court did not abuse its discretion in ordering the condition and concurred the defendant's conduct and protection of the community were appropriate reasons to order the condition.

Because of the uniqueness of these types of crimes, it will be the probation officer's job to inform the court of possible adjustments related to the offense and the use of a computer that are not already defined by specific computer enhancements. U.S.S.G. § 3B1.3. (Special skill) and more than minimal planning (in some chapter 2 specific offense characteristics) appear to be the adjustments/characteristics that are the more obvious for computer offenses. Other possible adjustments might relate to the use of a juvenile "hacker" by an adult (§3B1.4, Use of a Minor) and the obstruction

Table 3
Common Computer Crime Terms

Cloning	Term used to described the interception of legitimate electronic serial numbers (ESN), which are later entered into a stolen cellular phones to permit their use. (An ESN is a unique number assigned to each cellular phone that is transmitted each time the phone is used. ESN permits the phone to be used and billed accordingly.)
Cracker	A hacker who gains access and destroys data, completes some other destructive act to the system or profits in some manner from the access.
Encryption	Term used for hiding information in a secret code. For instance, encrypting a file so that it can not be read or interpreted until it is decoded. A file can be encrypted and then hidden inside another file (See steganography below). By doing so the very existence of the file is hidden and if detected it still cannot be interpreted until it is decoded.
Hacker	Originally coined at MIT in 1960's to refer to a computer expert. Now used to define individuals who gain unauthorized access to computer systems.
Hot or Test Keys	Performs certain pre-set security functions when touched that either make data inaccessible, unusable, or reverse the process to restore it. A "booby trap."
Logic Bomb	Software program that when certain factors are present will execute particular functions, i.e., the destruction of data or systems. One offender placed a logic bomb on a system that was designed to delete certain systems if his employer ever removed his name from payroll records.
Phreaker	Hacker who predominately gains access to telecommunication systems. (Note: Use of "Ph" is a play on the word phone, common in the hacker community)
Salami Method	Computer program used in embezzlement schemes to "slice" a small portion of the proceeds (i.e. $.01) from numerous accounts or payments and place those proceeds into the control of the offender.
Sniffer Programs	Software program that is placed on a computer system to surreptitiously function as an electronic wire-tap by intercepting the keystrokes and resulting system responses of users. The results are written as a file for later review to obtain passwords and account identification.
Social Engineering	Use of social skills to deceive others into disclosing information or providing services that an individual is not entitled.
Spoofing	The mimicking or counterfeiting of legitimate Internet protocol, frequently used to obtain information to gain unauthorized entry into systems.
Steganography	The science of hiding information in another medium. For instance, a child pornography image inside another image file. It is practically impossible to detect such a concealment.
Trojan Horse	Software program used to hide more nefarious or destructive programs.
Virus	Software program that "infects" other computers and takes over the system for a variety of functions ranging from minor manipulation of programs to wholesale destruction of systems and data. Virus "infection" is by someone either willfully or through negligence placing the program onto a system.
Worm	Software program that is similar to virus, with the exception that once created the program can self-replicate itself and "infect" other systems without someone actually placing the program on the system. Worms can attack networks.

of justice enhancements (§3C1.1) for offenders who use "hot keys" or "test keys" to destroy computer evidence (see Table 3).

Conclusion

The computer is becoming a weapon in the arsenal of the everyday criminal. Drug users are becoming more sophisticated by using computers to keep track of "customers," shipments, and money. Hackers are shutting down university computer systems, airports, and other systems, sometimes resulting in millions of dollars in losses and the threat of fatalities. As a new century begins, so does the problem of computer criminals for the probation and parole system. The training of officers in technical aspects of computer investigations and support software will become a vital part of an effective probation office. Many excellent training programs are now available through such organizations as SEARCH (http://www.search.org/, accessed 05/30/2001); the Federal Law Enforcement Training Center (http://www.fletc.gov/, accessed 05/30/2001); the High Technology Crime Investigation Association; (www.htcia.org, accessed 05/30/2001) and the National White Collar Crime Center (http://www.cybercrime.org/index.html, accessed 05/30/2001). It appears that as these problems become more prevalent, the necessity for some probation officers to become technical experts in computers will be inevitable.*

As criminals and their *modus operandi* change, so must the probation officer. We suggest officers who have the desire to excel in this area seek out training to become more educated in the computer arena. As the future unfolds, it may be common to have one or a handful of computer- literate probation officers specializing in the supervision of computer offenders. Not only can a computer-skilled probation officer supervise computer offenders, but he/she can also work in tandem with other specialists to further the effective supervision and investigation of all offenders.

As the 21st century commences, the supervision of computer offenders will become a common occurrence. The question for the probation field is whether we will be supervising them effectively due to preparation and training, or whether we will be attempting to catch up because we did not capitalize on the opportunity to address the issue earlier.

*Many offices across the country are also developing computer expertise. A few notable examples are: Southern District of Indiana, Middle and Southern Districts of Florida, the District of Columbia, Northern District of Ohio, and Western District of Texas.

References

Administrative Office of the United States Court, Federal Corrections and Supervision Division Center. (1998) *Internet Resources for Probation and Pretrial Services Officers*. Washington D.C.

The Associated Press (July 13, 2000). "Hacker Kevin Mitnick Allowed Back Online." www.nandotimes.com.

Bowker, Arthur (Spring 2001). "Providing a Frame of Reference: Lay Examples of Electronic Storage." *National Cybercrime Training Partnership Newsletter.*

Bowker, Arthur and Drinkard, Len (1996). "Downloading: Using Computer Software as an Investigative Tool." *FBI Law Enforcement Bulletin*, 65/6, 1-6.

Brunker, Mike (May 2, 2000). "Stiff Penalties Sought For Computer Crime." *MSNBC*, www.zdnet.com.

Cadigan, Timothy (August 3, 1998). "Officers Are Making Good Use of the Internet." *News and Views*. Administrative Office of the United States Courts, Federal Corrections and Supervision Division. 23(16).

Collette, Paul (April 24, 2000). "Monitoring Offenders' Internet Activity." *News and Views.* Administrative Office of the United States Courts, Federal Corrections and Supervision Division. 25(9).

Davis, L., McShane, M. & Williams, F.P. (1995). "Controlling Computer Access to Pornography: Special Conditions for Sex Offenders." *Federal Probation*, 59(2), 43-48.

Durkin, Keith (1997). "Misuse of the Internet by Pedophiles: Implications for Law Enforcement and Probation Practice." *Federal Probation*, 61(3), 14-18.

Fields, Gary (May 5, 2000). "Congress to Address Cybercrime Sentencing." *USA Today*, www.usatoday.com.

Painter, Christopher (March 2001). "Supervised Release and Probation Restrictions in Hacker Cases." *United States Attorney's Bulletin*, March 2001, Vol. 49, No. 2

Siuru, Bill (January/February 1998). "Tracking (or Trekking) Across the Internet." *Corrections Technology & Management,* 40-43.

Steve Jackson Games, Inc. v U.S. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), aff'd, 36 F. 3d457 (5th Cir. 1994).

Stored Wire and Electronic Communication and Transactional Records Access, 18 U.S.C. §§ 2701-2771.

The Privacy Protection Act, 42 U.S.C. § 2000AA.

United States Attorney's Office of the Northern and Southern Districts of Ohio (1998), *Practical Problems in Searching and Seizing Computer.*

U.S. Parole Commission, *Procedures Manual* 28 CFR §2.40-22.

U.S. Sentencing Commission (1996). *Guidelines, News from the U.S. Sentencing Commission*, August 1996, 8.

U.S. Sentencing Commission (1996). *Report to Congress: Adequacy of Federal Sentencing Guidelines Penalties for Computer Fraud and Vandalism Offenses*, June 1996.

U.S. Sentencing Commission (1996). *Report to Congress: Sex Offense Against Children, Findings and Recommendations Regarding Federal Penalties,* June 1996.

U.S. Sentencing Commission (1998). *United States Sentencing Commission Guidelines Manual*, November 1998.

U.S. Sentencing Commission, *United States Sentencing Commission Guidelines Manual*, November 2000.

United States Sentencing Commission, *Supplement to the 2000 Guidelines Manual.*

U.S. v. Crandon, 3rd Circuit, (1999), No. 98-5161.

U.S. v. Godman, 6th Circuit, (2000), Electronic Citation: 2000 FED App. 0261P (6th Cir.)

U.S. v. Hibbler 1998, Electronic Citation: 1988 FED App. 0317P (6th Cir.).

U.S. v. Mitnick, Central District of California, Case Nos. CR-603-MRP and CR 96-881-MRP.

U.S. v. Petersen, 1998, 98 F. 3d 502.

U.S. v. Williams, 1992, 966F.2d555,558-59, 10th Cir. 1992.

Wang, Wallace, *Steal this Computer Book: What They Won't Tell You About the Internet*, (San Francisco: William Pollack, 1998)

PACTS^{ECM}

Timothy P. Cadigan
Chief, Program Technology and Analysis Branch
Administrative Office of the U.S. Courts

ON APRIL 1, 2001 the federal judiciary began implementing the Probation and Pretrial Services Automated Case Tracking-Electronic Case Management System (PACTS^{ECM}). The result of years of planning, requirements definition, design, development, and testing, this implementation will position the federal probation and pretrial services system to utilize the technological tools of an advanced case management system on a daily basis. This article looks at the many implications and issues arising from a task of this magnitude and explores what the future can hold once this technological base is established. Areas of discussion include the application itself, design and development issues, implementation issues, potential benefits, business process change issues, and an exploration of future potential.

The PACTS^{ECM} Application

The PACTS^{ECM} system is both a case tracking and a case management tool. The case tracking component (PACTS) allows officers to electronically collect pertinent case-related information to produce statistical and workload reports. The case management portion (ECM) helps officers collect, manipulate, and recall case-management-specific information. This promotes more efficient and effective defendant/offender supervision and investigations for the district. Overall, the PACTS^{ECM} makes information more easily accessible to an expanded number of users and allows those users to manipulate the information in a manner more consistent with the professional activities they perform.

PACTS^{ECM} is a "total" information system. It includes functionality for: 1) electronic generation, storage, and retrieval of all investigation and supervision case information; 2) electronic retrieval for judiciary personnel of vital case information, including the presentence report, pretrial services report, and chronological records; 3) integrated access to the criminal component of the Case Management-Electronic Case Files (CM-ECF) project; and 4) electronic imaging of defendants/offenders—their tattoos, homes, vehicles, or other appropriate images.

The project team has worked closely with automation staff, data quality analysts, officers, supervisors, and administrative support staff from many districts to ensure that users' needs are addressed and that operational requirements are reflected in the data structure and user interface of the new Informix-based system. The intended audience for the PACTS^{ECM} application is the entire staff of probation and pretrial services offices. Probation and pretrial services operations involve approximately 7800 authorized positions in 509 locations. There are 93 district headquarters probation offices, 56 of which are combined probation and pretrial services offices and 37 of which have separate pretrial services offices.

PACTS^{ECM} is a browser-enabled application that is accessed through the federal judiciary's Intranet. It replaces its predecessor, PACTS Unify. However, it has been enhanced in two significant ways. The first is by expanding and redesigning the data structures in the database and the second is by using contemporary software tools and web technology. The enhanced database structures allow multiple IDs to be stored for each client. It also permits maintenance and search of historical sentence and historical address information. The software tools make it possible for PACTS^{ECM} to have graphical navigational tools such as drop-down lists and tabbed dialog boxes, display digital images, and link to resources outside the database. For example, the application links directly to Mapquest.com to provide officers with point-and-click access to directions to the defendant/offender's home.

The major features included as part of the first version of the software are a utility to make data conversion easier for data managers, a defendant/offender module, a treatment module, a pretrial services module, and a probation module. A number of standard reports and forms are available and the application provides for the required statistical extractions. Functionality will be added with Versions 2–4 of the software in generally the following order:

1. Automated Chronological records (Chronos);
2. Drug detection event tracking;
3. Completion of all forms and other "canned" reports;
4. Probation/Pretrial Services Case Plans and Reviews;
5. Fine and restitution tracking;
6. On-Line Case Assignment;
7. PS-2 Pretrial Services Interview Worksheet;
8. Electronic Monitoring;
9. Presentence Report Disclosure Tracking;

and

10. Interfaces to other databases including the FBI's National Crime Information Center (NCIC) 2000.

Design and Development

In-house development had been the normal mode for software development projects in the judiciary virtually throughout its history. At the time PACTS[ECM] was ready for development, the judiciary had recently been using off-the-shelf (COTS) software, with modifications for accounting and personnel applications, but all case-related systems had been produced internally, including PACTS-Unix, used in most probation and pretrial services offices. The proposal for development of the PACTS[ECM] application combined the strengths of both the in-house and outsourced development strategies previously used. The approach provided the necessary resources to complete the project in a timely manner and reduce the impact of other judiciary automation efforts on the timely completion of PACTS[ECM]. The judiciary was able to take advantage of substantial short- and long-term cost-saving opportunities, and the AO could effectively respond to requests from court users for enhanced automated functionality to manage the judiciary's vital information resources.

By using both in-house and outsourced talent, the PACTS[ECM] project team combined institutional and technical knowledge unique to the judiciary with a body of expert technical skills and knowledge in Informix and other state-of-the-market programming tools using the judiciary's Informix contract and other government agency contracts as needed. Combining resources in this manner allowed managers to reliably and more flexibly schedule highly skilled technical staff on the project—i.e., place the right people with the right skills on the right tasks at the right times.

This development approach was attractive because it made use of the considerable expertise and experience in the AO and in court units, including a cadre of in-house development personnel who are well-trained and productive, using fourth-generation languages (4GLs). In addition, federal pretrial services and probation offices (as distinct from state and local jurisdictions) offered considerable institutional knowledge and experience that no contractor could approximate, let alone duplicate. Finally, hourly labor costs of in-house personnel were lower than the most inexpensive contractor resources. Therefore, we used the contractor labor (which was considerably more expensive than the in-house labor) sparingly and only when necessary.

PACTS[ECM] Implementation

The PACTS[ECM] system is being deployed in a test wave of 14 courts, beginning on April 1, 2001. Recurring waves of 6 to 8 courts are scheduled to start at two-month intervals beginning February 1, 2002. Each wave will cover a nine-month implementation period. Prior to the start of the first wave in February 2002, changes in implementation will be made as appropriate based on the experiences of the test wave.

PACTS[ECM] implementation occurs when 1) applicable district staff are trained to use the PACTS[ECM] application; 2) technical tasks concerned with hardware and software installation and operations are successfully completed; and 3) the legacy database is converted to PACTS[ECM]. *The PACTS[ECM] Implementation Kit a*ssists the district by providing guidance, checklists, activities, suggested actions, and examples of documents, and provides the district with references to resource materials available through the J-Net.

The kit is divided into three sections: "getting started," "operations," and "systems," based on the nature of the activities covered and the intended audience. The "getting started" section is of interest to all participants. It lays the foundation for implementation. The "operations" section focuses on activities leading up to district staff being able to use the system. The target audience for this section includes chief probation and pretrial services officers, deputies, supervisors, data quality analysts (DQA), training specialists, and any officers assigned to assist in implementation. The "systems" section, which provides guidance on hardware, software, and database issues, is of most interest to the district's systems manager and systems staff. However, the "operations" and "systems" areas overlap. Decisions made by operations personnel will affect the work systems personnel must do to set up and support the system. Similarly, the systems staff expertise with supporting automated systems will be useful to the operations staff as they make key decisions or perform implementation activities. The district PACTS[ECM] project manager and the systems manager work closely together to ensure the successful implementation of the system.

Implementation Tasks

Perhaps the most useful tool within *The PACTS[ECM] Implementation Kit* is the PACTS[ECM] Implementation Project Plan. The project plan is a Microsoft Project file that can be used by district management as a quick reference to the tasks that must be accomplished in order to successfully implement PACTS[ECM]. Tasks can be checked off as they are completed, thus showing what has been accomplished and what is left to be done. The chief probation and pretrial services officers should meet with their district PACTS[ECM] project manager on a weekly basis to review the status of the project plan. The project plan also contains recommended start and end dates for each task, the anticipated duration of each task, and a time-line for the tasks. At the beginning of the implementation period, the district's PACTS[ECM] project manager will have received a copy of the project plan customized with dates appropriate to that district's start date. Each district has a PACTS[ECM] Implementation Coordinator from the Systems Deployment and Support Division (SDSD) within the Administrative Office assigned to support it in the implementation effort. The PACTS[ECM] Implementation Coordinator works with the project manager to track progress according to the customized plan. The district's PACTS[ECM] project manager may also wish to use the customized plan to manage the project using the Microsoft Project software.

Data Conversion— A Critical Cross-Functional Activity

Before a district can begin using the new PACTS[ECM] as its tracking and case management system, the data stored on the old PACTS-Unify system must be transferred, or "converted," to the new PACTS[ECM] system. The physical transfer of the data is a largely technical task performed by the district's systems staff as the last step before beginning live operations on the new system. However, a great deal of preparation needs to be accomplished early in implementation to ensure a smooth conversion of data. The most time-consuming task for most districts will be "cleaning" the data stored in PACTS. This task can begin as early as possible in implementation and is a collaborative effort between operations and systems personnel. Data-conversion software necessary for performing this task is supplied to the districts.

Training

Training for PACTS[ECM] is comprised of two primary components: application training for end users and technical training for technical staff who must support the application. The end-user training includes a train-the-trainer segment, as the majority of end-user training will be conducted in each district by district personnel who participated in the application training course defined here.

The PACTS[ECM] Application training course is designed to provide the necessary understanding and skills for the end user to successfully apply the newly-developed PACTS[ECM] software. Informational and introductory sessions will explain the enhanced functionality. Participants will be guided through the browser-based menu and on-line help links and develop an understanding of how the application applies to probation and pretrial services. Participants will also be prepared to deliver training to in-court personnel. The target audience includes data entry clerks, data quality analysts (DQA), and training specialists who will be responsible for training the remainder of the office staff. The course teaches participants to:

- Identify differences between PACTS[ECM] and the former PACTS Unify system;
- Confidently docket events on Pretrial and Probation cases;
- Create and modify client records and related events for both pretrial services and probation;
- Learn to generate reports and utilize on-line forms; and
- Incorporate PACTS[ECM] training materials into the court's training plan.

The class is delivered in two distinct components designed to accommodate both separate and combined pretrial services and probation.

The technical training is comprised of several classes: 1) Database Administration, 2) Systems Administration, and 3) Informix SQL. All technical training classes are provided in San Antonio, Texas at the judiciary's information technology training center.

This Database Administration course is designed to provide probation and pretrial systems staff with the technical information required for implementing and operating PACTS[ECM]. The course includes overviews of the application (modules, contents, navigation, enter data, query data, etc.), physical hardware/software architecture, and logical application architecture of DB schema. It identifies tables that will require local population and maintenance and review procedures for managing these tables. It discusses linking to resources outside the DB, implementation of login security algorithm, and maintenance of the NT and report servers and software. Finally, it presents security issues and the relationship of WordPerfect templates and Crystal Reports templates to report server software.

The systems administration course is intended for Informix Dynamic Server and Informix Dynamic Server system administrators. Participants learn the skills necessary to successfully administer one or more database servers: configure and initialize a database server instance, configure and test client connectivity, configure and manage memory and disk usage, plan and implement system maintenance tasks, and configure the server for optimal OLTP or decision support.

Finally, Informix Structured Query Language (SQL) course covers the Data Manipulation Language (DML) portion of SQL. Participants learn to create SELECT, INSERT, UPDATE, DELETE, LOAD, and UNLOAD statements, simple and complex joins, and subqueries. In addition, the course covers the basic configuration of an Informix instance, logical and physical log maintenance, archiving and restoring, and troubleshooting of basic configuration problems.

Benefits of The PACTS[ECM] System

The PACTS[ECM] system offers both intangible and quantifiable benefits to the end user or to the public at large. Intangible benefits are those benefits that are real, but difficult or impossible to quantify accurately or precisely. The quantifiable benefits have been assigned cash values.

First, as probation officers and pretrial services officers use PACTS[ECM] as a tool in their daily duties, paper waste should be reduced. The intention is to move to an environment in which the workstation becomes the usual medium for disseminating information, with a paper copy printed only on demand. However, it is difficult to predict human behavior: one manager may demand a paper copy of virtually everything, while another will be content with electronic dissemination of documents. Thus, we make no attempt to project savings in paper.

Second, and probably more important, but even more difficult to quantify, the accuracy and effectiveness of services should be increased by a benefit that, for lack of a better name, can be called data quality. PACTS[ECM] will increase data quality in two ways:

1. *Elimination of data redundancy.* This has two aspects:
   - The PACTS[ECM] database, using a fully relational database management system, will eliminate to as large an extent as possible redundancies of data.
   - The forms producing capability of PACTS[ECM] will integrate discrete data elements with form templates, thus eliminating the need to re-key data into multiple sources.
2. *Increased validation of data.* This will mainly be accomplished through use of standard tables for the various codes, and through cross-validation of user inputs based on the business rules (e.g., detention hearing date cannot be earlier than initial hearing date).

Third, increased efficiencies in productivity of probation and pretrial services officers will free them from their paper-intensive world to dedicate their energies to conducting more thorough and complete investigations, implementing better supervision practices, insuring community safety, and improving enforcement of pretrial release and sentence conditions imposed by judicial officers.

Fourth, the PACTS[ECM] information system will place the judiciary in a better position to respond to the grievances of victims, and to coordinate and share information with other law enforcement agencies. Although neither of these uses is part of the charter of the PACTS[ECM] project, both are benefits to the public at large that will accrue. They are not quantifiable, but they are real. The presence of a coordinated, validated, up-to-date information system from which details about federal probation and pretrial services defendants/offenders and their offenses can be quickly and accurately retrieved will increase efficiency, accuracy, and timeliness over the current manual methods.

Quantifiable benefits of the PACTS[ECM] system fall into two general categories: increases in efficiency specifically related to forms production; and increases in general efficiency. Tables 1 and 2 illustrate how even very modest cost avoidance associated with forms production and increases in general productivity can produce dramatic results

when multiplied across the entire user community. To demonstrate the possible efficiencies that could be achieved with PACTS^{ECM}, the project team traveled to the Western District of Texas probation and pretrial services offices to conduct testing comparing current methodologies of document production and PACTS^{ECM} methodologies of electronic forms development. Participating in the testing were staff from the AO's Systems Deployment and Support Division, Applications Maintenance and Development Division, and Federal Corrections and Supervision Division, and the probation and pretrial services offices from the Western District of Texas. Separate testing was conducted in each office.

The group agreed to test five forms for purposes of this analysis. Those forms are the initial case supervision plan (ICSP), travel permit, Form 14-A Request for Arrest Record, Flash Notice Request, and Form 7A Conditions of Supervision. These forms were selected by the group because of their frequency of use and because they ranged in complexity from a simple one-page form to the more elaborate multi-page case plan. The goal of the testing was to develop a base of knowledge to generalize to all forms without performing testing on all forms.

That testing demonstrated a wide range of average efficiencies achieved through the electronic forms development methodologies of PACTS^{ECM}. For example, the mean time for completion of the case plan was 36 minutes using the older methodologies. The mean time using the electronic forms development methodologies of PACTS^{ECM} was 6 minutes, a per-plan savings of 30 minutes. Simpler forms like the travel permit and Form 7A achieved smaller savings of 5 minutes and 10 minutes respectively.

The group agreed to test five pretrial services forms for this analysis. Those forms are the initial case supervision plan (ICSP), field sheet, Form 14-A Request for Arrest Record, initial chronological record, and PS 7 Reporting Requirements. These forms were selected by the group because of their frequency of use and because they ranged in complexity from a simple one-page form to the more elaborate multi-page case plan.

That testing demonstrated a wide range of average efficiencies achieved through the electronic forms development methodologies of PACTS^{ECM}. For example, the mean time for completion of the ICSP was 38 minutes using the older methodologies. The mean time using the electronic forms development methodologies of PACTS^{ECM} was 9 minutes, a per-plan savings of 29 minutes. Simpler forms like the field sheet and initial chronological record achieved smaller savings of 9 minutes and 7 minutes respectively.

The testing described above demonstrates the potential savings that can be achieved in probation and pretrial services offices when applying PACTS^{ECM} methodologies. Because we could not test every form used by officers, we generalized from the testing done in the Western District of Texas. The following table contains efficiency improvement estimates based on the number of cases handled in the system annually multiplied by the average number of forms per case multiplied by a conservative estimate based on our testing of 3 minutes saved per form. Those efficiencies are then given a dollar amount by multiplying the hourly rate of staff, in an effort to demonstrate the potential real efficiencies that can be achieved.

Table 1 presents a *very conservative* estimate of the savings that can be realized through the implementation of PACTS^{ECM}. The testing we conducted, which showed substantially more savings than we present, was artificially optimistic in favor of the current methodologies. In real life, staff time would be spent assembling the pieces of information necessary to complete the various forms. In PACTS^{ECM} all that basic information will be assembled instantaneously by the system.

Our analysis investigated the effects of three levels of hypothetical improvement in general efficiency.

- *Low improvement* is defined as a 1 percent improvement in overall efficiency of probation and pretrial services officers, and a 2 percent improvement in overall efficiency of support staff.
- *Medium improvement* is defined as a 2 percent improvement in overall efficiency of probation and pretrial services officers, and a 5 percent improvement in overall efficiency of support staff.
- *High improvement* is defined as a 5 percent improvement in overall efficiency of probation and pretrial services officers; and a 10 percent improvement in overall efficiency of support staff.

For example, a 1 percent increase in general efficiency among all officers, and exclusive of any efficiencies gained among support personnel, would yield a net savings (cost avoidance) of $3.12 million. For clerical staff a 2 percent increase in general efficiency would yield an annual cost avoidance of $1.56 million. The combined cost avoidance of officers and support staff would yield an annual cost avoidance of $4.68 million.

This analysis used the most conservative parameters; we have included the more optimistic figures here for the purposes of illustra-

TABLE 1
Increased Efficiency Through Electronic Forms Development

	Number of Cases	Average Number of Forms	Total Forms per Year	Savings per Form	Minutes Saved per Form	Hours Saved	Hourly Rate of PSO	Costs Avoided
PRETRIAL SERVICES								
Investigation Cases	63,497	5.10	323,835	3	971,504	16,192	$30	$485,752
Supervision Cases	30,502	10.04	306,240	3	918,720	15,312	$30	$459,360
TOTAL		15.14	630,075		1,890,224	31,504	$30	$945,112
PROBATION								
PSI/PSIG	49,826	10.80	538,121	3	1,614,362	26,906	$30	$807,181
Supervision Cases	88,966	13.16	1,170,348	3	3,511,043	58,517	$30	$1,755,522

tion, and because we believe the assumptions of 1 percent for officers and 2 percent for support personnel to be quite conservative.

Note that *cost avoidance* is not equivalent to *cost savings.* The cost avoidance due to increased officer and clerical efficiency will free those resources to perform other mission-critical aspects of their job. Thus, because the personnel will remain on staff, the benefits described in this document attributable to PACTS[ECM] are not actual savings to the judiciary. Rather, they demonstrate the costs avoided in freeing the probation and pretrial services community from their heavily paper-based environment. The benefit—quantified herein as cost avoidance—accrues not to the bottom line on a budgeting statement, but to the community that the federal judiciary serves. That community avoids the costs of inefficient and cumbersome manual procedures, and increases the effectiveness and perhaps also the range and scope of services provided by probation and pretrial services: ensuring the public safety, monitoring and supervising defendants and offenders, ensuring that conditions are met, and that violations are dealt with speedily.

TABLE 2
Savings Due to Increases in General Efficiency

OFFICER EFFICIENCY				
Hours Saved per Year	Average Hourly Rate	Savings per Officer per Year	Number of Officers	Total Savings per Year
20.8	$30	$624	5,000	$3,120,000
41.6	$30	$1,248	5,000	$6,240,000
104.0	$30	$3,120	5,000	$15,600,000
SUPPORT STAFF EFFICIENCY				
Hours Saved per Year	Average Hourly Rate	Savings per Clerical per Year	Number of Clerks	Total Savings per Year
41.6	$15	$624	2,500	$1,560,000
104.0	$15	$1,560	2,500	$3,900,000
208.0	$15	$3,120	2,500	$7,800,000
TOTAL EFFICIENCY IMPROVEMENT				
Rate	Officer	Clerical	Total	
Low	$3,120,000	$1,560,000	$4,680,000	
Medium	$6,240,000	$3,900,000	$10,140,000	
High	$15,600,000	$7,800,000	$23,400,000	

Business Process Changes

Achieving the benefits of PACTS[ECM] requires more than just installing software and conducting training. It requires a commitment from the chief probation and/or pretrial services officer to change local processes to take advantage of the functionality provided. The introduction of a new computer system into a work environment generally causes some disruption to day-to-day operations. Staff must learn new screens and commands, workflow may need to be changed, conversion of data and customized features from the old system is usually time consuming. All of this must happen while the office continues to accomplish its primary mission. In order to mitigate some of this disruption, tasks designed to ease the transition for data quality staff have been included in the PACTS[ECM] Project Plan. Most of these tasks are covered in two sections of the project plan, Business Processes and Training and Support.

Although PACTS[ECM] will replace the legacy case management systems in each of the federal courts' probation and pretrial services offices, each probation/pretrial services office has the flexibility to decide how the system will be integrated into the office's work processes. Three basic options are available, with unlimited local variance among them possible: 1) traditional data entry model; 2) officer-centric model; or 3) hybrid model combining both approaches, as shown in the table below.

The choice of the implementation strategy is a management decision that will directly affect the business processes and workflow within the office. To assist management in making this decision, a Business Process Workgroup could be formed to document current business processes in a manner that is easy for managers to review, understand, and modify. Once current processes have been documented and reviewed and the business process model has been chosen, the Business Process Workgroup can prepare the office to begin day-to-day operations using PACTS[ECM] with the process model chosen for that district.

Depending on the model chosen and the degree of change from the current model, the district will have to re-engineer business processes to insure a smooth transition. For example, having officers enter data will introduce more error into the data entry process. Therefore, management needs to create or modify the district's data quality assurance plan and procedures to reflect the new workflow. That quality assurance program would need to compare entered data to source documents, look for common errors, and report back to staff who make errors on those errors so that staff can become aware of them and avoid similar errors in the future.

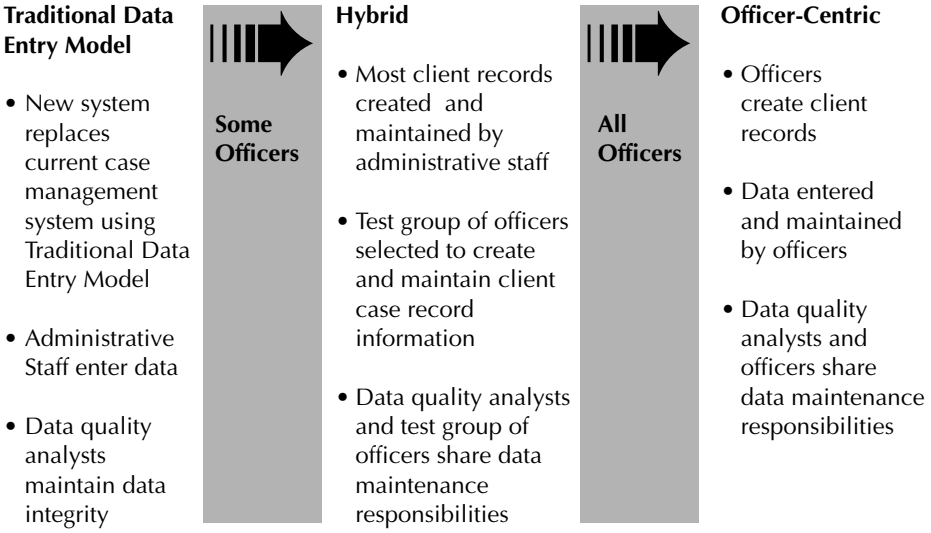
The simple fact that the current process is changed could cause the district to establish procedures that are not now necessary. For example, opening up the data entry function could introduce the possibility that cases get lost before they get entered. This has obvious negative implications for workload credit for the office. Therefore, it may be necessary to validate and make any necessary adjustments to new work processes after the PACTS[ECM] system has been implemented to insure against this type of problem.

One final obvious area that will clearly need to be reviewed *encompasses several areas including all local forms, reports, and applications. For example, it may be necessary to modify data collection forms to reflect the new screens and to accommodate the new workflow. The district should also work with the systems staff to determine the need for existing locally developed reports and applications. This analysis should look carefully for any duplication of effort between PACTS[ECM] and the local system which preceded it.*

The Future

The probation and pretrial services user community has long desired and sought support for the development of automated functionality that empowers officers in the community. That desire first manifested itself in the Mobile Computing project, which tested the idea of using laptops to provide that functionality. That project demonstrated the value of

TABLE 3
Range of PACTS^{ECM} Business Process Model Options



technology when the officer was away from the office. However, it also demonstrated the limitations of bulky laptop computers in providing that functionality. The expanded use and functionality of personal digital assistants or handheld computers has raised the probation and pretrial service community's interest in meeting their needs through these devices. As PACTS^{ECM} begins implementation, the District Court Technology Panel and Chiefs Advisory Group believe strongly that the Community Technology initiative is the most important need of officers on the street. The objective of this project is to provide probation and pretrial services officers with the automated functionality they need to more efficiently perform the duties required of them by law in the community. The project will focus on using this technology in five critical areas: pretrial services supervision of defendants; post-conviction supervision of offenders; presentence investigations; pretrial services investigations; and safety of officers in the community. Federal probation and pretrial services officers are required to investigate and supervise defendants/offenders as ordered by the court. Those functions require officers to leave the courthouse and go into the community. Therefore those officers are "remote knowledge workers" requiring electronic access to case-specific data from a variety of remote locations. Moreover, the primary concern of the judiciary and officers in the community is the personal safety of officers in the field. Those two needs combined create the need for officers in the community to have handheld computers.

Another potential source of integration is with kiosk technology. The kiosk could collect a live biometric measurement of offenders' hand geometry or fingerprints or one of several other options to verify that the offender is the one interacting with the kiosk. Then, the screen would prompt the probationer to answer a series of questions (in English or Spanish) previously determined by the probation officer, including current address, phone number and other information. The kiosks could also collect fine and restitution payments. Once the electronic reporting session is complete, the system issues a receipt to the probationer. Over time, a detailed history of the degree of compliance is collected on each offender. The system identifies those who are non-compliant, and for whom the probation officer may need to take some direct action.

The future of technology in the field of community corrections is only limited by one's ability to conceive effective uses for the ever-growing waves of technology to the field of community corrections. Harnessing that potential while eliminating those technologies that are more toy than useful tool is the secret to success in these initiatives. However, having a "state of the market" case management system is the first and most essential step in implementing these various technologies in a community corrections system. With the implementation of PACTS^{ECM} the federal probation and pretrial services system is poised to move forward on a solid foundation.

The Chief as a Technology Manager

Michael Eric Siegel, Senior Education Specialist, Federal Judicial Center
Elaine Terenzi, Chief U.S. Probation Officer, Middle District of Florida

THE PROBATION OR PRETRIAL services chief who wishes to fulfill the mission of federal probation and pretrial services—"to exemplify the highest ideals and standards in community corrections"—will find in technology a powerful, but sometimes mysterious, ally. Though the benefits of using technology in the probation/pretrial services field are compelling, the difficulty of making it work is still troubling and, for some, seemingly insurmountable.

The first challenge for chiefs, then, is a *mental* one—to believe in technology, not as a panacea for all the challenges in the system, but as a helpful tool to accomplish their daunting responsibilities and to manage their complex operations. Chiefs should strive to be, or to become, "believers" in technology, thereby rejecting the alternative postures that include "waverers," "atheists," "agnostics," "zealots," "hypocrites," and "monarchs" (Earl and Feeny, 2000: 11-16).

What will make chiefs believers? First, understanding the extent to which information technologies are changing our patterns of commerce, organizational design, social interaction, and work. Chiefs should consider the following facts:

- Over the past decade, the portion of new capital investment devoted to information technologies has risen from under 10 percent to over 50 percent, making it the largest category of capital investment in the U.S. economy by far.
- Banking transactions over the Internet cost only about 3 percent of those at traditional walk-in counters, suggesting the huge productivity gains possible from delivering services over computer networks. (Harvard Policy Group, 2000: 1)
- When Bill Clinton first entered office in 1993, there were only 50 web sites in the entire world. Near the end of his administration, however, he reported that there were nearly 20 million sites on the Internet (Clinton, 2000).
- Through the efforts of the recent project on Reinventing Government, federal executive agencies have used technology to achieve significant progress in their performance. For example, passport applications are now available on the Internet, and the 1-800 service of the Social Security Administration outperformed L. L. Bean and Disney in 1995 (*Blair House Papers,* 1997: 5).
- In the judiciary's own time line (developed at the request of Congressman Harold Rogers), before 1972 there was virtually no automation to support the federal judiciary's core functions except electric typewriters. By 1998, the judiciary had a national communications network linking 30,000 employees at 700 sites. It also had installed the Federal Judiciary Television Network, which, by 2000, had some 250 downlink sites across the nation, making it the second largest government satellite network in the U.S.
- According to this same report, the benefits of technology for the judiciary's probation and pretrial services officers include technological tools and capabilities such as mobile computing, immediate access to criminal databases, ankle monitors and remote electronic monitoring, and on-site urinalysis—all to enhance the investigation and supervision of offenders and increase public safety. (AO and FJC, 2000: 32).

The logical conclusion of this mountain of evidence on the importance of technology in our personal and professional lives is that "a posture of disengagement is now outdated" (Harvard Policy Group, 2000: 2). Assuming that a chief will choose to be a believer in technology, what is the next hurdle to overcome? The second challenge is a *strategic* one, as chiefs consider how to fully exploit the benefits of technology, instead of simply using it to automate high-volume bureaucratic routines. The goal of automation is to use networks to enhance productivity and improve services. In short, chiefs must learn how information technology can be used for strategic innovation and not simply for tactical automation.

Consider, for instance, the potential power of mobile computing. Probation and pretrial services officers spend two to three days a week in the field performing investigative work or client supervision. Mobile communication, including cellular telephones, pagers, laptop computers, tablet computers, or personal digital assistants, can increase officer productivity—and safety—considerably (AO and FJC, 2000: 32).

Most districts have developed report-generating assistance for officers assigned to conduct presentence investigations. Numerous versions of macro-generated reports assist officers in developing a well-organized and thorough report with limited assistance from support staff. The Southern District of Florida

uses an offender telephone call-in system as a means of monitoring their administrative caseload. The information is automatically entered into a searchable database, which highlights changes in an offender's reported circumstances for follow-up by an officer or assistant.

Chiefs should also consider the potential power of a handheld computer instrument. As viewed by Chief Terenzi:

> Handheld computing instruments, such as the Palm Pilot, offer a whole new dimension to portability solutions. Just within the past few months this new tool has become the one item I can't manage without! It is loaded with a searchable database containing identification information, address, and case management information for all 3500 offenders under the supervision of our offices (downloaded from PACTS and automatically updated with each "HotSync"); all active investigations in the district, to whom they're assigned and when they are due; the Administrative Office and Federal Judicial Center directories; and an emergency contact list for all our staff including home, office, cell, and emergency contact numbers. I now carry a library of reference materials in my wallet. It includes our district manual, our local rules, Title 21 and Rule 46 of the U.S. code, the DSM-IV, a drug identification reference manual, the 2000 U.S. Sentencing Guidelines, and the Guideline and Criminal History Calculator. I can use it to track my travel expenditures, check my calendar, and have it remind me of important meetings. All this, and I have used less than half of its available memory! A Global Positioning System (GPS) can be added to help find your way in the field; bar code scanners can be added to quickly process inventory, file systems or U/A samples. The tool seems only limited by our imaginations.

Having developed a strategy to take advantage of technological aids, the chief faces the challenge of *implementation*—making things work. Perhaps the most important dimensions of this challenge are the development of excellent relationships with systems staff and the evolution of effective management strategies to manage and develop automation staff. Like other executives, chiefs are sometimes frustrated in their work relationships with automation professionals. Part of the frustration stems from the fact that automation professionals see the world quite differently from probation/pretrial services chiefs, and yet the contributions of the automation professionals to the work of probation and pretrial are vital, as indicated above.

The MOHR Company conducted research on the working preferences and characteristics of technical professionals during the 1980s and 1990s. MOHR interviewed thousands of automation professionals in high-technology companies, such as Hewlett-Packard, IBM, and Apple Computers. They concluded that technical professionals exhibit the following kinds of characteristics:

A Desire for Autonomy

Technical professionals prefer to select the conditions, pace, and content of their work. They are a highly credentialed group of employees, with notable marketable skills, and they bristle at the idea of being micro-managed. Indeed, technical professionals may harbor suspicions of management, or remain confused about what managers actually do. When asked to describe a perfect working world, they frequently mention a work environment devoid of managers entirely.

A Need for Achievement

Technical professionals enjoy solving difficult problems. They are delighted when they have an opportunity to apply their specialized skills to solve complex problems or develop innovative solutions. They tend to become energized by figuring things out; in fact, sometimes they become excessively involved in a project, losing their ability to focus on any competing priorities. Technical professionals welcome uninterrupted blocks of time when they can concentrate on solving problems and developing or enhancing programs. Unfortunately, this need for achievement does not always translate into providing outstanding customer service.

Professional Identification First, Organizational Identification Second

Like university faculty, technical professionals identify strongly with their "discipline" and only secondarily with their organization. One of the authors vividly remembers attending faculty cocktail receptions (which he does not recommend) where he would discover the disciplinary identifications of several new acquaintances (economist, sociologist, etc.) and only later in the conversation understand their organizational affiliation (The University of Maryland, The University of Chicago, etc.). Similarly, in the courts, automation professionals are more likely to identify with the computer community and less so with the court community, or in the case of probation pretrial, with the criminal justice or community corrections communities.

Participation in Organizational Mission and Goals

While technical professionals may not immediately identify with probation and pretrial work, they will be more highly motivated to do so through explanations of the "business" and its goals than through incomplete political statements like, "The boss just wants it done!" Technical professionals resist internalization and commitment to mandated organizational goals, preferring to rely on logical and goal-oriented justifications. Moreover, research conducted even more recently than the MOHR studies indicates that technical professionals want to feel that they make a difference in organizations; they want to feel part of a larger purpose. As expressed by Wall Street Journal reporter Kemba Dunham:

> Today scores of managers and professionals are fleeing their jobs in the for-profit dot-com economy for more personally rewarding—but usually less financially remunerative spots in the non-profit world. (2000)

Collegial Support and Professional Development

Technical professionals, as mentioned, are interested in making positive contributions to their organizations. They want to be perceived as part of the organization, not as standing apart from it. They want positive feedback when they have done good work. In this regard, they are like all other employees. Moreover, technical professionals are in a profession where obsolescence is common; they, more than most others, are in desperate need for continuing education and even certification opportunities. (MOHR Development Co.: 5)

There are things chiefs should and should not do in order to bring out the best in their systems staff. If we could imagine a systems manager describing what she would like to have from her chief (and what she would not want from her chief), the ideas would read something like this:

> I know you cannot give me a full grant of autonomy, because we are both responsible to the court and to the citizens of this

nation. Consequently, I will have to learn more about the schedules, deadlines, and process of probation and pretrial. I will have to familiarize myself with key events and with the issues of volume of caseload, types of caseload, supervision needs, and all the rest. That way I will know how I can contribute more in the first place.

I do not, however, work well in environments where I feel that people are constantly looking over my shoulder, second-guessing me, and, ultimately, not trusting me to do the right thing. I look forward to receiving projects and work assignments from you, but I would like a chance to discuss them with you in order to gain a better understanding of what you're really trying to accomplish. I want to know which of the projects are urgent, and which can be done at a more relaxed pace. I also would like to have input into these matters when possible.

I am driven by a sense of achievement, and although I don't always show it, I would like to contribute meaningfully to this agency. In this regard, I am interested in sitting in on management meetings, even though the scope of those meetings extends beyond automation issues. After all, if you're calling me a "systems manager," I ought to identify with the management of the district or office.

Conversely, systems managers need to understand the responsibilities of the chiefs. When we look at the organizational and cultural perspectives of chiefs, we can quickly identify a potential for "disconnects" with technical professionals. Chiefs desiring to create an autonomous work environment for systems staff might be prevented by the deadlines and the rhythm of the judicial process. When there is a large-scale arrest besetting a pretrial services office, a chief cannot endure delays caused by her systems staff being unavailable to help due to its involvement in rewriting code. In terms of the justifications for change and project development, it is not always as rational a world as the systems staff would like. Politics intercedes, and the chiefs must mollify judges who are not generally known for their patience.

In order to manage successfully the many tasks for which the chief is responsible, the systems manager can be a powerful ally. The following might be a chief's perspective on what she hopes from the systems manager:

I have a wide span of responsibility and accountability, and I have different time constraints than you. I have to interact, not only with those within our office, but with other agencies and organizations. I need information to be summarized. At the same time, I am not as technically literate as you, and need to have some things explained in more detail.

It will help both of us if you understand the nature of the work that my other staff do and the pressures under which we operate. For instance, a defining aspect of offender supervision in the federal system is the practice of using individualized supervision plans for each offender to achieve the multiple goals of enforcing court orders, enhancing community protection, and successfully reintegrating offenders into the community. Managing individual plans for 50 to 70 offenders while conducting pre-release investigations, responding to collateral assistance requests from other districts, and managing a variety of legislative requirements for special offenders is a tremendous organizational challenge. To juggle all of this while spending most of his time in the community can make an officer feel as if he is on a treadmill broken in the "on" position. The interrelated aspect of each segment of supervision may seem confusing to you. However, by looking at the whole picture, you might be able to understand that solutions that make sense when looking at a single issue or challenge become impractical in the fast-paced, fluid world of supervision services.

Moreover, the supervision officer cannot be tied to a desk. To be effective, the officer must be in the community where the offenders live, work, and oftentimes violate the conditions of their release. These officers struggle to find the time to learn a new computer system or program. They are reluctant to type their own work. Their lack of interest in these desktop tools can be frustrating to the technical professional designing them.

In terms of our presentence officers, whom I also supervise, their investigation assignments are quite high. The deadlines come faster with even more investigations behind the ones they are currently working on. They are like Lucille Ball wrapping and placing chocolates on a constantly moving conveyor belt, on that famous TV sitcom episode. When a presentence officer needs assistance, it often comes with a proverbial scream and not much patience: "I NEED IT NOW!" If taken personally, this could damage the relationship with you, the technical professional (who feels unappreciated); thus, the request could be misinterpreted as an unreasonable demand (presentence officers are spoiled and impatient).

I also need your help in understanding some of the challenges I face in maintaining a sense of fairness for all of my employees. For instance, as the salaries of the technical professional increase, and in some cases surpass, those of the hazardous duty staff they serve, animosity can get in the way of partnerships. From an officer's perspective, technical staff do not perform the core work of the probation service and should not be compensated at a level higher than an officer. From their view, the disparity in formal higher education between the two professions only adds salt to the wound. Officers are required to have a bachelor's degree at a minimum and many have master's degrees. Technical staff, on the other hand, often pursue certifications rather than degrees and may not be as adept at communication in writing or around a conference table as an officer.

Also, officers, especially presentence writers, are acutely aware that they work for the court and embrace the tradition of the court as an important part of their culture. Their dress is conservative and their manner professional. Technical staff, on the other hand, consider themselves to be part of the probation office. They are not "sworn in" before a judge as an officer of the court. But you need to contribute to a professional working environment, especially by way of your appearance. Therefore, I have to be fair in expecting everyone to dress in a conservative, professional manner, in a way that reflects the nature of our work.

In order to bridge this gap of understanding, the chief must be creative. To help systems staff become acquainted with the officers' work, she can have the staff open a case, dictate a chrono, conduct a case review, and prepare a court packet. Arranging for an automation professional to ride along with a probation officer for a day would help the automation professional appreciate the complexity of the job and also the benefits of mobile computing to officers' success (and safety). In this way, they will see the strategic uses of technology in addition to its bells and whistles.

The chief can also be an advocate for the technical staff—taking the opportunity to champion their attributes to the officers, publicly recognize their creativity, and explain the highly obsolescent nature of their profession. For example, by posting the number and frequency of support calls to which technical staff must respond, the chief can point out that, like probation and pretrial services of-

ficers, automation staff must be adept at multitasking.

Furthermore, the chief needs to develop a certain level of trust in her automation staff to gain the full benefit of their productivity. To realize the benefits of technology in a strategic way, as discussed earlier, the chief has to relinquish whatever tendency he has to micro-manage automation staff. This grant of autonomy to automation staff may seem threatening to chiefs, who usually are in close control of office operations; however, in the realm of technology, chiefs usually do not have sufficient expertise to maintain close control. And, again, technical professionals will work more productively when trusted by their managers.

In sum, to maximize the benefits of probation and pretrial services, chiefs and systems managers must bring their special talents and strengths to the collective enterprise of management. As Peter Drucker once said, "Management is about human beings. Its task is to make people capable of joint performance; to maximize their strengths and render their weaknesses irrelevant" (1988: 75).

Conclusion

In a March 1997 interview with *Government Technology*, Kathleen O'Toole, then Massachusetts Secretary of Public Safety, described the progress made in her state to integrate the various components of the criminal justice system (1, 42, 44). With the state's "single inquiry system," police, probation, corrections, and parole officers can access a large database of information from a variety of state agencies. A single inquiry on a subject at a traffic stop, for instance, could turn up outstanding warrants, restraining orders, probation and parole status, court records, DUI arrests, sexual offender records, and firearms registration. She noted that "many of the agencies that we needed to interact with to accomplish this totally integrated system fell within different branches of government" (1997: 42). Nonetheless, the agencies cooperated to overcome "turf wars," because they were united in the vision of a fully integrated criminal justice system to help reduce or respond to crime in Massachusetts.

Technology makes this kind of seamless system a real possibility for the federal probation and pretrial system as well. To benefit from its use, probation and pretrial chiefs need to believe in technology, develop a plan to use it in a strategic fashion, and implement the plan through collaborative relationships with all staff members.

References

Administrative Office of the U.S. Courts and the Federal Judicial Center. "Technology and the Federal Courts: The Role of Technology in Federal Court Operations and Education, Now and in the Future." October 2000. Jointly submitted to Congressman Harold Rogers, Chairman of the House Appropriations Subcommittee on Commerce, State, the Judiciary and Related Agencies.

Clinton, Bill. "Remarks by the President in Internet Webcast." 22 September 2000. 2000 White House Press Releases and Statements. At <http://www.ed.gov/PressReleases/09-2000/wh-0922.html>. 23 January 2001.

Dunham, Kemba J. "As Sites Struggle to Stay Afloat, Internet Employees Choose Higher Calling of Charities." *Wall Street Journal,* 5 December 2000.

Drucker, Peter E. "Management and the World's Work." *Harvard Business Review*, September-October 1988: 65-76.

Earl, Michael and David Feeny. "How To Be a CEO for the Information Age." *Sloan Management Review*. Winter 2000: 11-16.

Harvard Policy Group. "Eight Imperatives for Leaders in a Networked World." JFK School of Government, 2000.

MOHR Development Co. *Technical Leadership: Managing and Motivating Today's Technical Professionals.* Stamford, CT: MOHR Development Co (undated).

O'Toole, Kathleen. (Interview.) "Building a Seamless Law Enforcement and Criminal Justice Newtork." *Government Technology*. Vol. 10, No 3, March 1997: 1, 42, 44.

President Bill Clinton and Vice President Al Gore and the National Performance Review. *Blair House Papers*. Washington, D.C.: 1995.

Wall Street Journal. "What Price Glory? Personal Tales of the Dot-Com Trenches." November 15, 2000, B1.

Pagers, Digital Audio, and Kiosk: Officer Assistants

Thomas G. Ogden, Deputy Chief
Cary Horrocks, Systems Manager
U.S. Probation and Pretrial Office, District of Utah

Introduction

Most officers will agree that the focus on offender contact field work has increased dramatically over the last decade. Officers need to spend their time and efforts on issue- and result-driven contacts. Officers must *triage* their efforts on the offenders who need immediate and multiple contacts to ensure public safety and compliance with court-ordered conditions and sanctions. Almost every district will indicate that officer "field time" has increased over the past five years. Officers are doing better jobs of planning and identifying issues to address at field contacts; nonetheless, increased field time does not always yield increased contact with the defendants/offenders or collateral sources. Officers still spend a great deal of time calling and driving to homes or work sites only to leave a card for the defendant/offender to call back. This equates to thousands of personnel hours, resources, and other support duties with great "issue-driven intentions" but no results. To be fair, many offenders/defendants also spend a lot of time leaving messages and wasting trips to the office only to find their officer unavailable.

Basic technology such as e-mail, fax, and answering machines have certainly increased communication and allowed transmittal of important information in an efficient manner. Those basic technologies are commonplace to businesses, but often not always readily available to offenders/defendants, especially the cases we need to see the most often. We must look at other available technologies that can facilitate contacts and field work without wasted efforts. The district of Utah implemented the use of digital dictation/transcription and traditional pagers as time-saving programs and is currently developing a kiosk machine. These programs are an effort to allow greater flexibility of work hours and create more time for *face-to-face* field work.

"Page me"

When looking for an employee who is not at their desk, we usually page or call a cell phone; we do not drive to their house or work site and hope they are there. Family members, children, and significant others carry pagers. Take a walk down the hall of any high school and it will appear that every other student has a pager. The reason for such popularity is that pagers are inexpensive and efficient. With the exception of a few isolated rural areas, a person can be contacted anywhere.

For the past three years, the district of Utah has found designated pagers to be an efficient way to contact offender/defendants without wasted trips, telephone calls, or other fruitless efforts. The pager is the property of the Probation and Pretrial Services Office and is assigned to the offender/defendant as a condition of supervision or pretrial release. Only the Probation and Pretrial Services Office knows the number, which keeps the defendant/offender from using the pager for personal calls. If the pager beeps, it is the officer with a directive. Offender/defendants are required to respond to the pager 24 hours a day, seven days per week.

Use of the pager can be designed by the individual supervision officer to meet the needs of each case. For example, if number "1" appears on the LED screen, it means call your officer immediately, "2" means come to the office within one hour, "3" means submit a urine sample within two hours, etc. The menu is only limited by the officer's imagination. Pagers have worked very well with offender/defendants who do not have or cannot afford telephones. Those defendants/offenders are most likely to cause an officer a great deal of fruitless effort to make contact. If paged, that offender/defendant can go to a public telephone or neighbor to contact the probation/pretrial office. Although the program works well in any area, it can be a great time and miles saver with rural caseloads.

Pagers have also served as an alternative or enhancement to traditional ankle-bracelet electronic monitoring. Current electronic monitoring can control and report a defendant/offender's movement at the home or base station. It does not assist the officer during the hours the defendant/offender is on work or other release from the transmitter station. The pager can contact the defendant/offender at any time and any place with directives from the officer. It is most often used as an enhanced sanction at administrative staffings or violation hearings for offenders/defendants who have demonstrated a need for more control.

Pagers are inexpensive and can be combined with offender/defendant co-pay or full pay as part of the special conditions, depending on local court policy and philosophy. The District of Utah originally leased the pagers for approximately $4.00 per month. The Probation and Pretrial Services Office subsequently purchased pagers, pays a lower monthly service fee, and issues them directly to the offender/defendant as ordered by the Court. Cost for replacement of the pager if lost, broken, or stolen is approximately

$60.00. At today's gas prices and other transportation-related costs, combined with the wasted hourly salaries for "no contact" efforts, the pagers appear to pay for themselves nearly instantly. Currently the offender/defendant signs an agreement to reimburse the cost of the pager if it is lost or stolen; but even in the few cases where the pager or money is not recovered, it is money well spent on the supervision mission. For any criminal supervision office, this technology can increase offender contact while decreasing the effort and time to successfully facilitate the contact, leaving more time for other issues and urgent field supervision activities.

Digital Dictation and Transcription

We all know "if it's not documented, it didn't happen." In support of that theory, the District of Utah has installed a digital dictation system. These types of systems have been used by doctors and police agencies for years to transcribe information at the end of an event or shift from any location. It allows officers and staff to enter chronological case notations ("chronos") from any telephone at any time. The officer can spend a full day in the field, go directly to his/her home or any telephone and call in the information. Officers dial into the systems and then are prompted for a user identification number, a work type, and a subject identification number. The records are then transcribed by support staff (who also can be located anywhere) and entered into the computer system with less than a two day turnaround.

Since implementing the digital dictation system, the District of Utah has received many benefits. Any officer who has had to cover or respond to another officer's case knows the importance of being able to have the most current activity available before making contact with the defendant/offender. This necessity is met with digital dictation since support staff can transcribe from any field office or alternative location (i.e., work at home). This allows for guaranteed quick turnaround entry without delay due to support staff being on sick or annual leave. This type of system also allows managers to create alternative work sites and make better use of traditional office space. It further allows management more equitable options for work distribution without the limitations of geography and distance.

In Utah, the majority of presentence reports transcribed for officers in the Salt Lake main office are completed by support staff in the satellite St. George office 305 miles away. Chronological records are transcribed by a clerk at a "work at home" alternative duty station. Digital dictation also creates the potential for part-time transcriptionist positions and other options for the maximum use of decentralized Court Personnel System funds.

Dictation transcribed from the digital system is entered and saved on the district computer network system with no greater delay than when working with support staff in the same building. There are no tapes to be transported, damaged, or lost. This system works for all written information stored by the Probation and Pretrial office. More importantly, it keeps officers in the field for investigations and offender/defendant management rather than behind a keyboard doing a clerical job at an officer's salary.

Active workload statistics can readily be extracted from the digital system to provide information on the amount of work to be transcribed or the amount completed. Turnaround time is easily computed for the information that is stored. Hourly work status graphs help evaluate and equalize work assignments for support staff.

What is a Kiosk?

The District of Utah Probation and Pretrial Office is currently developing a plan to involve kiosk technology as an aid to supervision strategies. We project the first kiosk to be up and running by November of 2001. We are all familiar with these *interactive machines.* Although nothing can beat good face-to-face customer service, it is nice to be able to do banking at 6:00 a.m. or 10:00 p.m. It is convenient to walk into your favorite book or music store to see if the item you are seeking is available, without having to wait in line or find one of the few available clerks. Some people actually prefer asking for information and doing business with a machine rather than live interaction. These machines have made our precious time more flexible and adaptive to our needs.

With a kiosk, officers enroll an offender/defendant and capture their fingerprints digitally with scanners from Identix. A user identification number is created based upon the PACTS number, and the fingerprints become the password to the system. An e-mail account is also created. They will be entered—with case-specific information—into the database.

When defendants/offenders use the kiosk, a biometric sample is taken (via scanner) and compared to the one collected during enrollment. Once a match is established, the offender/defendant can interact with the kiosk by pressing buttons on the touch screen. Data is entered to verify address and employment status and to respond to questions defined by the probation officer. The probation officer may also send messages for a defendant/offender to be delivered the next time he/she checks in at a kiosk. The defendant/offender can read the mail message and respond electronically. Written instructions are given on screen. A digital photo of the face will be captured. When the session is done, a receipt is generated for the defendant/offender's records.

Utah plans to place the first kiosk in the lobby of the current federal Community Corrections Center (CCC). This will provide line of sight supervision by CCC staff to avoid vandalism and abuse. The future may hold unlimited placement options such as police stations, malls, or any business willing to host or lease space. It will further facilitate convenient interaction and use by offenders/defendants reporting to CCC for drug testing or other court-ordered functions.

What the Kiosk Can Do

The kiosk permits us to expand but not replace our role as officers while providing alternative service solutions. It frees the officer's time for field supervision as it automates tasks such as mandatory in-office reporting and Monthly Supervision Report (MSR) collection. It can increase defendant/offender accountability while decreasing routine officer tasks. Our district feels there are numerous applications to *enhance* defendant/offender contacts within the scope of supervision. These applications are not designed to *replace* defendant/offender contact; the kiosk is a support tool for *enhancing* the supervision officer's role, not a *robot* supervising offenders/defendants.

Defendants/offenders can receive specific information from their probation/pretrial services officers that is confirmed by picture and fingerprint identification. With a PIN or ID number defendants/offenders can receive specific reporting instructions (when, where, what to bring) from their officer. As with the pager, this type of system would work very well with defendants/offenders who do not have a telephone. Currently for those with telephones, there is "plausible denial" with

answering machines and leaving messages with collateral sources. Offenders can claim the answering machine is broken or was erased, or the person answering the phone never gave them the message. With the kiosk, the probation/pretrial services office can assure the information was available, correct, and in working order and received by only the defendant/offender. The responsibility of getting the information is transferred to the defendant/ offender rather than being on the officer. Most would agree that placing more responsibility on defendants/offenders to meet their obligations is a *desired outcome* of supervision.

With the kiosk's ability to transmit information, unlimited assistance can be given to defendants/offenders. The information can be specific to the defendant/offender for his/her eyes only via fingerprint access, or could be general information that all users can view. Bus routes to and from the courthouse, local job service, counseling centers, etc. can be accessed by the touch of a screen. Counseling and treatment schedules can be available with all current changes. Job opportunities with where and how to apply could be entered and updated from the main office. Again, the information to be transmitted to the defendant/ offender is only limited by the officer's or district's imagination.

The kiosk would also be useful for agencies that track mandatory felony reporting. Often felons on travel status are required to go to a police station, wait in line, and then present identification to an officer/staff member to meet the requirement. The felon is then allowed to leave with no other instructions. The kiosk, with fingerprint verification and prompted questions, could streamline this procedure and, more importantly, could have the information immediately entered and transmitted to police, probation, and pretrial services agencies.

The kiosk is also a two-way street. Defendants/offenders can provide and transmit information to probation and pretrial services officers. MSRs, lists of places the defendant/ offender applied for work, address changes, lease agreements, etc., could all be transmitted to the appropriate officer immediately. Although answering machines can do some of this now, the kiosk provides more specific information in printed format. The officers could receive the information the next working day to verify activities and to facilitate the planning of their field work. It could also speed up the required PACTS entries for address changes. Depending on placement of the machines, it could prevent defendants/offenders needing to take time off work to meet their obligations of probation and pretrial release. The last thing any officer wants is defendants missing work or losing a job over absenteeism when they are compliant in all other areas.

The Kiosk and Pretrial Supervision

The kiosk is particularly useful in providing pretrial services officers with a reasonable assurance strategy for monitoring risk of nonappearance. Defendants on travel permit status can check-in upon return at anytime with visual verification. Defendants can be required to check in on weekends or during non-traditional hours, thus limiting the ability to engage in unauthorized travel for any significant distance. Judges and magistrates may become more confident with the ability to monitor defendant travel and order pretrial release on cases that may have been detained in the past. Furthermore, this *could* free up jail space and temporary housing for higher risk cases.

The kiosk will also serve as an additional amended strategy at violation hearings to diminish the risk of nonappearance. Here again, offering increased sanctions on violation cases could enable judges to keep marginal cases on supervision rather than in detention. This would save the often-scarce jail beds for those offenders posing a more serious risk of harm to the public.

The principal focus is to maintain contact with defendants who pose a manageable risk to the public and who require moderate personal supervision. If used in conjunction with personal face-to-face reporting, the defendant can come to the department office once per month, and report to a kiosk once per week for the rest of the month. Administrative or compliant caseloads of defendants who pose little or no risk to the public can report as needed to receive and transmit information. Again, this does not supervise our compliant caseloads with "robo cop" but rather enhances our contacts with that portion of our caseloads in an efficient and timely manner. The kiosk will increase contact and control of cases, not replace the officer's job. In the spirit of least restrictive pretrial supervision, the kiosk is considerably less restrictive than reporting to a courthouse or pretrial services office and offers more flexible hours.

System Components

The kiosk is designed with durable metal construction cabinet and a powdercoat industrial finish to protect against graffiti and vandalism. User interfaces consist of an Elo 17-inch touch-screen monitor, vandal-resistant keyboard, Identix biometric scanner, Practical Automation ATX 38 printer, Visioneer Strobe Pro scanner, and digital camera. Processing is done by a PIII 1Ghz CPU with Windows 2000 Professional. Kiosk systems are manufactured by several companies. Kiosk Information Systems was chosen to build the system for Utah. The kiosk structure is an ergonomic design to allow easy screen access. Attention was given to screen position and height to allow handicapped persons access and to be compliant with the 1992 Americans with Disabilities Act. An open-frame standard monitor was chosen over the new TFT flat screen displays. This choice was made because the Elo 17-inch screen gave better readability and was less costly. The system is connected to the kiosk server via a VPN connection. The kiosk server is a PIII 1Ghz CPU with Windows 2000 server and SQL 2000. An Identix biometric scanner is attached to be used for enrollment. Crystal Reports is used to produce standard management reports and specialized form generation.

Conclusion

Using technology for officer assistance is not optional to remain a successful and competitive agency. Probation and pretrial services supervision will always require logical thinkers to make subjective decisions to achieve and fulfill the mission. Officers cannot be replaced by machines. The gadgets and machines listed above can assist and give us more time to complete the subjective and personal duties of jobs.

Endnotes:

The following are web sites related to the technology in the article. The philosophical and mission-related applications of the technology are the opinion of management in the District of Utah Probation and Pretrial Office.

www.identix.com
www.crystaldecisions.com
www.fmakiosks.com
www.elotouch.com/partners
www.kis-kiosk.com
www.automon.com
www.visioneer.com
www.dvi.com
www.metrocall.com
www.practicalautomation.com
www.publicaccesskiosks.com
www.kiosk.com

Remote Location Monitoring—A Supervision Strategy to Enhance Risk Control

Darren Gowen, Chief, Integrity and Safety Section
Federal Corrections and Supervision Division
Administrative Office of the United States Courts

HISTORY WILL show that at the close of the 20th century, community supervision's "best practices" for verifying compliance with court-ordered release conditions called for officers to personally check on their offenders[1] at home, work, and other locations. Offender compliance was also typically verified by officers speaking with family members, treatment providers, and employers, and by reviewing pay stubs, sign-in logs, and time sheets.

History will also show that in practice, community corrections had scarce resources and a concomitant profile of desk-bound officers and crowded reception rooms of offenders and defendants waiting to report to their assigned officers.

The 21st century holds many promises for humankind. Perhaps it also holds the promise of resolving the question of how community supervision can be both effective and efficient. This article explores cost-effective technological solutions to this banal problem in community corrections. No longer do we have to keep one foot in the past century and the other foot in the current one. Application of remote supervision technologies can help us make that final step. The future of community corrections has arrived!

Background

In 1998 the Federal Corrections and Supervision Division and a workgroup of U.S. probation and pretrial services officers began exploring technologies that officers can use to remotely monitor the physical location of an offender. For example, home-based electronic monitoring (EM) is often used by officers to remotely monitor offenders who are restricted to their homes.[2] A popular alternative technology uses a system that identifies offenders over the telephone with a voice verification technique.

The workgroup's study of remote supervision technologies sprang from issues encountered while developing policies and procedures for the federal home confinement program. While it is common to refer to home confinement as EM, the latter term actually refers to only one technological tool for monitoring a participant's compliance with some of the rules of the home confinement program.

While focusing on the technological tools currently used in the federal home confinement program, workgroup officers began focusing conceptually on ways they could perform their jobs more effectively without increasing resources. Coining the concept, *remote location monitoring,* the workgroup officers defined its purpose as improving the officer's ability to maintain awareness as a necessary first step in controlling and addressing defendant/offender risk.

With the home confinement program, an officer's primary task is to monitor and verify an offender's location at all times. But even when offenders are not participating in the home confinement program, there are typically other conditions of supervision that may require them to show for required appointments, conduct a job search, and maintain regular employment. An offender's compliance with some of these required activities can be more effectively and efficiently monitored remotely by the supervising officer.

This is not to make a case against officers spending time in the field checking on their cases, or reviewing documents. What remote monitoring adds to this traditional mix is an inexpensive way to monitor compliance when it is supposed to occur, rather than finding out about it at some later time. The application of remote location monitoring should free the officer's time so that the traditional functions are more purposeful and focused.

Remote location monitoring requires technological systems, such as EM, voice verification, and other tracking systems that can verify a person's physical location, either periodically or continuously, 24 hours a day. Location monitoring systems provide a tool to verify–in real-time—a person's whereabouts for specific risk issues or court-ordered release conditions. In this way, technology aids the officer in effectively satisfying specific supervision functions without loss of officer efficiency.

Risk-related Applications

Which technology to use for remote location monitoring should depend on the apparent risk that an offender presents to the community. Higher risk cases obviously require tighter monitoring parameters. Remote supervision technologies can be categorized into three risk-related applications: Random/Programmed contact systems, hybrid systems, and GPS monitoring systems.[3]

Random/Programmed contact systems can address a broad range of supervision risk-control issues. Such systems are typically comprised of automated telephone contact systems that require the subject to call-in or receive a telephone call, followed by a process of identification and location, usually through voice identification methods. The automated verification contacts can be configured to provide frequent and random con-

tact verifications at multiple locations.

Example: An offender wears a pager. Each time the pager beeps, the offender calls from the nearest approved telephone. This could occur while the person is at home, at work, or elsewhere. During the verification call the system prompts the offender to repeat a series of words or phrases. The system compares the spoken words or phrases to a voice template created during the system enrollment. A successful matching between the offender's voice and the voice template positively identifies the offender. The officer sees the results on a computer screen showing a successful voice identification and the telephone number from which the identification took place.

All current automated telephone contact systems require the officer to enroll the participant, set and revise schedules, review data, and—for pager-initiated call-ins—distribute and maintain equipment. Even with these added tasks, the automated contacts still provide a significant time reduction over the officer contacting the offender by conventional means.

Hybrid systems combine the EM and a programmed contact method like voice verification. The EM verifies the person's location while at home and the programmed contact system periodically verifies the location when away from home. The *programmed contact*s substitute for the officer's telephone calls or in-person field visits to monitor the person's compliance with an approved schedule and location. Possible applications for hybrid systems include the following:[4]

- Adding voice monitoring to EM to address increased risks that may be related to a participant's location while away from home.
- Using programmed contact to verify an offender's locations that are varied or distant, making frequent community visits by the officer difficult.

Global Positioning System (GPS) satellite monitoring is a technology that has the capacity to continuously map the exact location of defendants or offenders. It also alerts the officer when participants venture into set geographically excluded locations or fail to be present at required locations at specific times of the day.

A GPS uses a network of 24 satellites to calculate the location of a GPS receiver. A link to a cellular telephone network allows the reporting of location to a monitoring center. In currently available systems, these components are housed in a small box that the participant carries by hand, with a shoulder strap, or in a fanny pack. To assure that the participant is close to the tracking/reporting systems, the participant also wears an ankle transmitter that reports to a radio receiver in the tracking/reporting system. It is similar to a conventional electronic monitoring system except that instead of being attached to a residential telephone, the receiver is attached to a cell phone interface that always knows its location because of data coordinates from the GPS receiver.

GPS monitoring provides continuous remote location monitoring to enforce specific court-ordered conditions without increasing labor costs. Like traditional electronic monitoring, the officer must set up a daily time schedule for the participant. But with GPS, the officer also incorporates geographical locations where the participant must be present at certain times as well as locations that are off-limits. For example:

- *Exclusion zones* can be designated for locations where the participant is prohibited, such as within physical proximity of a victim or potential victim.
- *Inclusion zones* can be designated for the participant to be present at a location for set time periods, such as an employment site. The inclusion zone verifies the participant's adherence to a location schedule.

Because GPS can signal when an offender enters a prohibited location, it can be used for persons whose risk is associated with an identified personal or institutional victim. Its continuous mapping features might also be used when a subject's adherence to strict physical parameters is not limited to the residence but presence in or absence from certain locations is a paramount supervision risk-control issue. Potential participants are limited by the current state of technology that requires the offender to carry the field monitoring device and perform a number of daily maintenance tasks.

Certain types of construction may block the reception of GPS signals. If a high-risk offender works in an office building sub-basement, the portable receiver unit (that the offender must carry) may not receive GPS signals. More common issues arise, however, with cellular coverage dead spots. Although a GPS receiver may continue to receive and calculate location coordinates, the ability of a portable monitoring unit to report may be sufficiently impaired in a few areas. The officer knows the offender's location only after the portable unit has successfully communicated GPS coordinates to a monitoring center, which in turn reports its information to the officer. Thus, the officer must weigh any cellular coverage limitations and potential GPS signal blockages against the type of risks presented by the potential participants.

Continuous remote location monitoring systems offer officers a different type of information about defendants/offenders. Alerts that the defendants/offenders are entering an "exclusion zone" may signal the potential of *imminent* danger to persons or groups, requiring a quick predetermined response from the officer. For this kind of monitoring, probation and pretrial services offices need to develop working agreements with local police who are capable of emergency response prior to implementing real-time tracking. Even then, officers need to verify cellular availability in exclusion zones. In addition, officers should make sure that the perimeter of any exclusion zone can be set wide enough to allow for proper response time to the actual "target." For example, in setting an exclusion zone for a domestic abuse victim, the officer estimates how long it might take the offender to travel from the zone boundary to the actual victim's home. However, unnecessary alert notifications could occur if exclusion zones encompass all elemen-

FIGURE 1
Levels of Remote Location Monitoring

Random/Programmed Contact to monitor evening curfew	Home-based Electronic Monitoring	Home-baseed Electronic Monitoring plus Random/ Programmed Contact System	Continuous Remote Location Monitoring using GPS

Lowest ← **Monitoring Level** → **Highest**

tary schools and child care centers but the offender's approved travel route crosses into an exclusion zone.

Use of the GPS for remote location monitoring presents a restrictive supervision condition that would generally require a court order. Setting inclusion and exclusion zones can be driven by court-imposed orders aimed at specific risks, such as travel, employment, associations, and contact with others. Setting parameters (zones) can also be determined by identified risk issues in the supervision case plan and requires methodical assessment by the officer.

Participant Selection

Where the home confinement program for postsentence offenders is primarily used as an alternative to prison for punishment purposes, remote location monitoring can focus on a particular case's risk to the community. Some examples of potential application include the following:

- Persons presenting third-party risks that have an identifiable victim, e.g., domestic violence or sex offenders—focus on exclusion zones.
- Persons presenting a flight risk but no specific victim. In such cases, GPS could be used with parameters set for a broad inclusion zone (city or county) and specific exclusion zones, such as airports.
- Drug defendants and offenders—tight focus on inclusion zones; exclusion zones. The officer can adjust exclusion zones as the participant's location patterns are discerned and suspect areas (e.g., high drug-trafficking areas) then also excluded to reduce community risk.

When officers look at potential participants, they should identify specific community or flight risks that this program can directly address—risks that other supervision programs, tools, or techniques cannot address effectively or efficiently. To further illustrate this, figure 2 presents some conceptual levels of remote location monitoring for designated levels of offender risks.

Information obtained through the use of GPS monitoring or other remote location monitoring technologies could result in some additional reasonably foreseeable risks for which officers would have a duty to warn an identifiable third party at risk. This situation might arise, for example, if an offender with a history of domestic violence is tracked to an area close to the residence of a person whom he has a history of abusing.

Figure 2
Conceptual Levels of Remote Location Monitoring for Designated Levels of Offender Risk

Level 1
is reserved for the highest risk pretrial defendants and postconviction offenders. It involves real-time tracking of set inclusion and exclusion zones and routes of travel. Use this level if the case has an identifiable victim or potential victim(s), such as a domestic abuse or sexual assault victim.

Level 2
is used for cases where there is no identifiable victim or potential victim but the case presents significant general risks to the community or flight, such as might be the case with a pretrial defendant with drug-related charges. This component allows the officer to receive next day mapping of participant locations rather than real-time coordinates. Component parameters include a larger inclusion zone (stay in this area or city) and specific exclusion zones (e.g., stay out of housing projects).

Application Levels 1 & 2 are reserved for the highest risk populations

Level 3
This level uses programmed contacts (e.g., voice monitoring) or hybrid (e.g., voice & electronic monitoring) systems to focus on inclusion zones only (not exclusion zones) for risk control purposes. Level three would not be appropriate for low-risk home confinement participants without any significant risk control issues.

The use of continuous remote location monitoring is likely to bring to light situations in which officers can reasonably be expected to react to protect a person or persons at risk. Program procedures, such as the sample notification schedule presented in figure 3, should incorporate appropriate responses from officers to lessen the community risk that may be presented by persons being monitored with remote location monitoring systems.

Remote Access to Monitoring

One key aspect of remote location monitoring is the number of work tasks the officer must perform to access and work with monitoring data and information. Most of the available monitoring systems provide remote access to their monitoring network via the Internet or terminal access. Remote access typically involves officers using their own properly configured computer, software, and Internet connections to exchange monitoring data (including enrollment, data/curfew changes, caseload review, reports, and terminations) with the monitoring center via secure access to a web site. Remote access increases officer efficiency by reducing data entry time, increasing accuracy, and providing real-time access to monitoring data.

Prompt and accurate officer notification of violations is a necessity for monitoring offenders. However, because notification requirements are commonly unique for each participant, basic notification processes traditionally have required human intervention, resulting in longer response times and decreased accuracy. Remote access to a monitoring system enables fully automated violation notifications to be sent to officers for each participant. The automated notifications can be configured to immediately page the officer with the participant's name, violation type, and time of occurrence. Other simultaneous or staged notifications could be sent to others (e.g., officer's supervisor, potential victim, or law enforcement agency) via pager or email.

Performance measurement is an essential component of any successful program. Remote access to monitoring systems provides officers the capability to track program statistics. A number of commercial systems provide customizable reports that automatically extract program statistics at the level of detail desired and format the information into customizable reports.

Remote access for officers enhances the managing of resources and identification of trends in supervision, and provides correctional agencies with an important tool to balance caseloads among line staff to monitor and improve program performance.

Figure 3
Sample Notification Schedule for GPS Monitoring Key Events

Key Event	Officer Alert Notification Schedule
Exclusion Zone	Immediate
Inclusion Zone	Variable
Equipment Tamper	Immediate
Proximity Violation	~5 min
Loss of Cellular Phone Contact	~ 10 min for level one participants; variable for level two.
Loss of GPS Signal	~ 10 min for level one participants; variable for level two.
Low Equipment Battery	Variable

Although remote access requires some technical and management skills on the part of the officer, the quick access to monitoring information aids officers in making more timely decisions that may ensure greater public safety.

Conclusion

The proper application of remote supervision technologies in supervision is a cost-effective way for officers to do a better job with the same or even fewer resources. Remote supervision technologies offer a reliable tool for officers to monitor compliance with location restrictions, such as those by which home confinement program participants must abide, or offenders who are given other travel or location restrictions as special conditions of court-ordered supervision. The elegance of this concept is that a particular remote technological application can be tailored on a case-by-case basis. Remote access to monitoring data eliminates many of the manual tasks officers previously performed with EM systems. Remote technologies are a critical component of community supervision in the twenty-first century.

Endnotes

1. Use of the term *offender* is used here as a generic reference to all persons under criminal justice supervision, including pretrial defendants.

2. Electronic monitoring systems alert the officer when a participant leaves a specific location, usually their residence, or tampers with the electronic monitoring equipment. The participants wear a waterproof, shock-resistant transmitting device around the ankle 24 hours a day. The transmitter continuously emits a radio frequency signal, which is detected by a receiving unit connected to the home telephone. When the transmitter comes within the signal range of the receiver unit, the receiver unit calls a monitoring center to indicate the participant is in range or at home. The transmitter and the receiving unit work in combination to detect and report the times participants enter and exit their homes. The electronic monitoring equipment only indicates when participants enter or leave the equipment's range--not where they have gone or how far they have traveled.

3. Although I provide a brief description of various technologies, my focus is on their application by officers. For a more detailed description of the available technologies, see Peggy Conway, *A Basic Introduction to Electronic Monitoring Technologies* in *Journal of Offender Monitoring*, volume 13, Number 1, winter 2000 pp.9-10,17.

4. Voice monitoring methods could be used in lieu of EM if the participant is a low-risk. This has the benefit of increased location monitoring but the trade off is lack of continuous monitoring when at home—programmed contacts while at home instead.

Reducing Alcohol-Related Crime Electronically

Kirby Phillips
Alcohol Monitoring Systems

ELECTRONIC ALCOHOL monitoring technology as a deterrent to alcohol consumption has been used for several years. However, truly cost-effective and reliable technology that operates as a 24-hour monitor has yet to be realized. This article proposes the implementation of a new technology, which monitors the excretion of ethanol through the skin as a measure of blood alcohol levels. This technology will provide those in community corrections with a reliable and effective means of assisting with the rehabilitation and policing of offenders sentenced to abstain from alcohol consumption.

The impact of alcohol use on our society has been widely researched, and the strong link between criminal behavior—especially violent behavior—and crime has been an issue of public policy concern for decades. Nonetheless, solutions to the disproportionate amount of resources, space, and dollars required for alcohol offenders in our overcrowded criminal justice system are diverse and controversial. According to the National Center on Addiction and Substance Abuse (CASA) at Columbia University, "Releasing drug- and alcohol-abusing and addicted inmates without treating them is tantamount to visiting criminals on society." In their 1998 report, *Behind Bars: Substance Abuse and America's Prison Population,* CASA goes on to state that of every dollar spent on substance abuse in state budgets in 1998, 96 cents went to "shoveling up the wreckage" of substance abuse and addiction, while only 4 cents went to actually prevent and treat it (CASA 1998).

In 1996, the American Probation and Parole Association issued a position statement on substance abuse treatment in community corrections. Based on research revealing that involuntary participation in treatment works approximately as well as voluntary participation (Anglin & Hser, 1990), the APPA states that, "Probation and parole is an effective context for treatment to occur. An integrated approach involving assessment, treatment-offender matching, intervention (i.e., treatment), surveillance (i.e., drug testing), and enforcement (i.e., sanctions) is an appropriate strategy for dealing with drug-involved offenders" (APPA 1996).

According to a 1996 study by the National Highway and Traffic Safety Administration, recidivism rates one year after sentencing of DUI offenders were 33 percent lower for subjects sentenced to a combined program that included home detention and electronic monitoring. Since offenders often fail to comply with all the terms of their sentence, NHTSA recommends investigating the costs and benefits of implementing various mechanisms to increase compliance with sanctions (NHTSA 1996).

The Price of Alcohol Abuse and Recidivism

The number one substance abuse crime in America is drunk driving, accounting for 1.47 million arrests in 1997 at a cost of over $5 million (Bureau of Justice Statistics 1999). Add to that the fact that as of the year 2000, America broke the $100 million-dollar-a-day barrier in spending to incarcerate individuals with serious drug and alcohol problems (CASA 1998).

Some additional facts:

- As a whole, according to CASA, alcohol is more closely associated with crimes of violence than any other drug, with 21 percent of state and 26 percent of jail inmates incarcerated for violent crimes under the influence of alcohol alone at the time of their offense (CASA 1998).
- One-third of all DWI offenders on probation and two-thirds in jail are repeat offenders. Over half of DWI offenders in jail were on probation, parole, or pretrial release at the time of their new offense.
- In terms of parole and probation violations, 50 percent of state parole and probation violators were under the influence of drugs, alcohol, or both when they committed their new offense (Bureau of Justice Statistics 1999).

The bottom line? Only a fraction of offenders who were alcohol abusers at the time of their offense, regardless of the offense, are ever actually sentenced to abstain from alcohol. On average, there are over 1.4 million DWI arrests annually, resulting in 513,200 DWI convictions. And while 33 percent of those convicted and sentenced to probation are repeat offenders, only 10 percent of them are actually ordered to abstain during the term of their probation (Bureau of Justice Statistics 1999). Many industry experts believe the current lack of an effective, affordable monitoring technology explains the large disparity between the number of convictions and the number of offenders required to abstain from alcohol.

With a philosophical shift toward rehabilitation to combat the impact of alcohol and drug abuse on crime, relief for those in community corrections is seen in recidivism. Whether a community corrections program

defines success by an increase in recidivism—and thus effective implementation of the policing function and protection of public safety, or by a decrease in recidivism—defined as an increase in compliance and rehabilitation—an effective surveillance method can support both objectives, serving as a deterrent for the offender and a reliable policing mechanism for community corrections.

Effective Surveillance

One factor that severely limits the ability of community corrections to establish cost-effective, comprehensive alcohol treatment programs is the availability of effective technology for monitoring court-ordered abstinence. Current technologies tend to be labor-intensive amidst a system that is already stretched to the limits, and the small number of tests leaves offenders with a wide window of opportunity for violation.

The most recent technology to enter the electronic-monitoring arena is transdermal testing, where an ankle bracelet monitors an offender's blood alcohol level by measuring the ethanol migrating through the surface of the skin. The goal of this new technology is to provide the corrections community with an effective alternative for monitoring offenders on a continual, 24/7 basis, and at a cost that is competitive with electronic home arrest proximity monitoring programs that are currently in place around the country.

Transdermal Testing Methodology

A number of independent scientific studies support the strong correlation between breath, blood, and transdermal alcohol levels. In 1985, Dr. Daniel J. Brown of the Department of Pharmacology and Toxicology at Indiana University School of Medicine published "A Method for Determining the Excretion of Volatile Substances Through Skin," which showed that the concentration of alcohol in insensible perspiration is not substantially different from that of breath or blood following complete absorption (Brown 1985). In 1987, *Alcoholism: Clinical and Experimental Research* published "Ethanol Vapor above Skin: Determination by a Gas Sensor Instrument and Relationship with Plasma Concentration," which concluded that skin vapor measurements are comparable to breath alcohol analyzer determinations, stating that the transdermal testing method "may be performed in situations where breath alcohol analyzer measurements are inconvenient or where continuous monitoring is desirable (H.G. Giles, et al. 1987)."

Based on this scientific foundation supporting the transdermal testing methodology, Colorado-based Alcohol Monitoring Systems has developed SCRAM—the Secure Continuous Remote Alcohol Monitor—which remotely monitors a subject using transdermal testing and delivers information from the offender to supervising personnel. Dr. Thomas Crowley of the University of Colorado Health Sciences Center conducted a test of the SCRAM proof of concept units, confirming that the alcohol readings of the units strongly correlate with breath analyzer readings.

The SCRAM Technology

The SCRAM system encompasses many of the principles of current electronic monitoring technology and is intended to function as one component of a comprehensive program. The system allows each monitoring authority to customize the method of notification for each individual offender, and the technology will work in conjunction with existing monitoring companies that are experienced users of comprehensive case management programs. Intended to function as one component of an intensive-supervision program, rather than an alternative, it can be used in pre-trial, pre-release, probation, supervised release, and parole settings.

The Monitoring Bracelet

The ankle bracelet has two small modules that are held on opposite sides of the subject's ankle by a tamper-resistant strap. Each module weighs approximately 4.4 ounces. The unit is waterproof and is designed to handle the stress of everyday activity. SCRAM's patented information technology automatically measures the subject's alcohol level on a schedule set by the supervising agency. The anti-tamper features included in the system make it difficult for monitored subjects to circumvent or distort readings, and the SCRAM system's patented tamper and interferrant gas detection processes ensure that supervising medical and probation officials can be confident that readings are from the proper subject and accurately represent a subject's blood alcohol level. The Monitoring Bracelet is designed to detect and record any tampering or attempts to remove the device.

The Smart Modem

The Smart Modem, which communicates test results from the subjects home to the Central Monitoring Station, also facilitates bi-directional communications between the Monitoring Bracelet and the Central Monitoring Station. The Monitoring Bracelet communicates with the Smart Modem via encrypted 900 mhz. radio frequency communications. Users may employ a curfew function that requires the subject to be at home (and within 50 feet of the Smart Modem) each day during a time determined by the case manager. At that time, the Smart Modem sends encrypted information to the Central Monitoring Station via a standard phone line. Alcohol readings, tamper alerts, and diagnostic data are all communicated to the Central Monitoring Station. In turn, the Central Monitoring Station uses the Smart Modem to download monitoring schedules, reporting schedules, and software updates to the Smart Modem and Monitoring Bracelet.

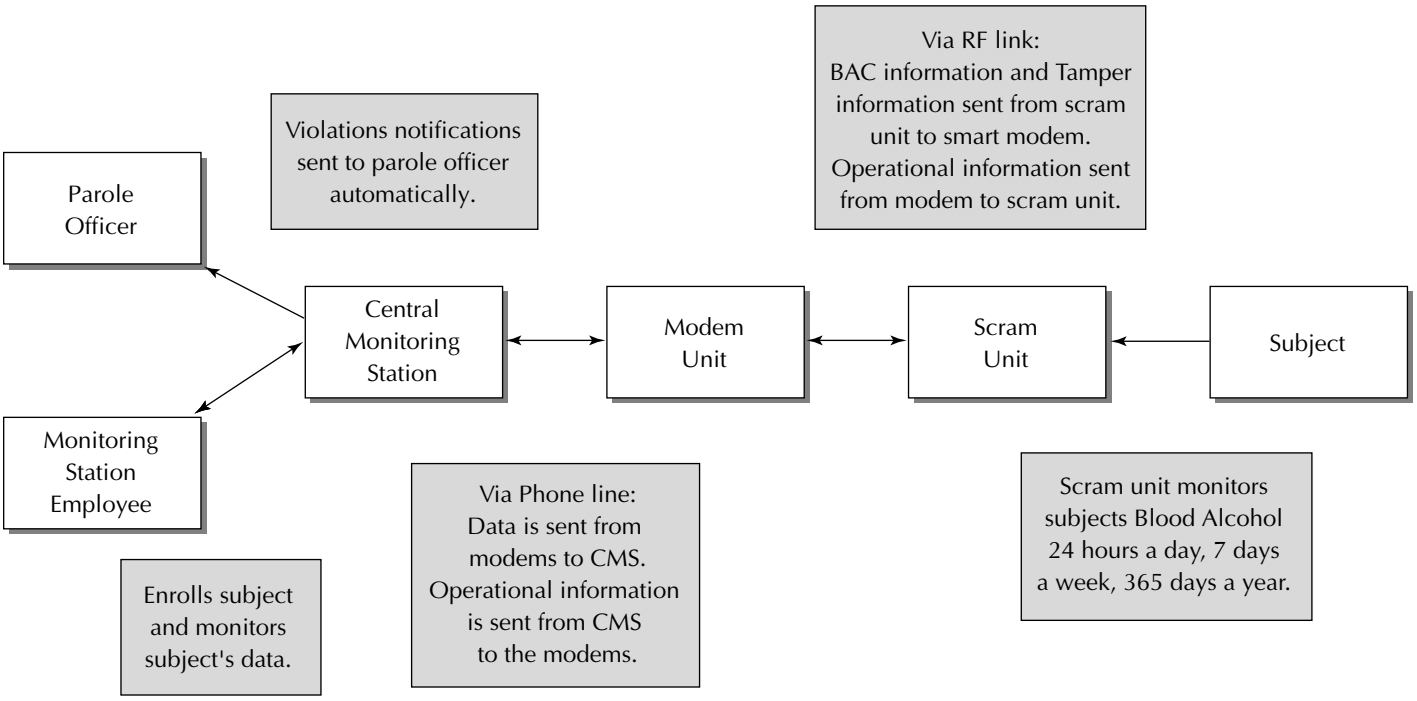
The Central Monitoring Station

The Central Monitoring Station is the control center for the entire SCRAM system. It allows the supervising authority to control the testing, synchronization, and reporting schedules for each unique monitoring subject. During the course of each day the Central Monitoring Station will notify the supervising authority of any positive alcohol readings, tamper alerts, or equipment malfunctions based on the reporting preferences of each case manager. The Internet-based Central Monitoring Station also provides supervising parties with 24/7-access to the alcohol readings of each subject. The supervising agency can print a variety of reports for periods of one day or one year. Figure 1 provides an overview of the system.

A Critical Element, a Comprehensive Solution

Today's conventional wisdom—and fiscal realities—all support the concept of change and rehabilitation. The National Institute on Drug Abuse estimates that, "for every $1 invested in treatment of drug-involved individuals, taxpayers enjoy a $4 return in the reduction of costs related to alcohol and drug abuse (NIDA 1992). A 1994 study in California revealed a $7 return for every $1 invested (National Opinion Research Center 1992)." CASA estimates that if only 10 percent of substance-involved inmates are successfully treated and trained, the economic benefit in the first year of work after release would be $8.6 billion. In addition, estimates of the

FIGURE 1
Scram System Block Diagram



number of crimes committed by each abuser range from 89 to 191 per year. At the conservative end, successfully treating and training just 10,000 addicts would eliminate 1 million crimes a year.

Developers of the SCRAM transdermal technology are careful not to position their electronic monitoring program as a complete solution. Instead, SCRAM is designed to work in conjunction with other program elements, including initial offender assessment and ongoing client evaluation, substance abuse treatment, home arrest, definitive consequences for violations, and graduated sanctions.

References

American Probation and Parole Association. (1996). *Position Statement on Substance Abuse Treatment.* American Probation and Parole Association.

Bureau of Justice Statistics (1999). Special Report: *DWI Offenders under Correctional Supervision.* (June 1999). Washington, D.C.: U.S: Government Printing Office.

Brown, Daniel J. (1985). "A Method for Determining the Excretion of Volatile Substances Through Skin." (1985). *Methodology and Findings in Experimental Clinical Pharmacology, 7(5), p. 269–274.*

Giles, H.G., PhD, S. Meggiorini, BSc, G.E. Renaud, J.J. Thiessen, PhD, E.I. Vidins, MD, K.V. Compton, V. Saldivia, BA, H. Orrego, MD, and Y. Israel, PhD. (1987). "Ethanol Vapor above Skin: Determination by a Gas Sensor Instrument and Relationship with Plasma Concentration." *Alcoholism: Clinical and Experimental Research, Vol. 11, No.3, May/June 1987, p. 249–253.*

National Center on Addiction and Substance Abuse at Columbia University (1998). "*Behind Bars: Substance Abuse and America's Prison Population.*" (1998).

National Highway Traffic Safety Administration (1996). "Traffic Safety Facts" (1996).

National Institute of Drug Abuse and National Institute on Alcohol Abuse and Alcoholism (1992). "The Economic Costs of Alcohol and Drug Abuse in the United States-1992" (1992).

National Opinion Research Center (1994). "Evaluating recovery services: The California Drug and Alcohol Treatment Assessment General report" (1994). California Department of Alcohol & Drug Programs, Sacramento, CA.

Interactive Video Training for Firearms Safety

Timothy M. Scharr, Senior United States Probation Officer
Special Offender Supervision Team, St. Louis, MO

IN 1998, 178 hazardous incident reports were reported to the Federal Corrections and Supervision Division, representing an increase of 52 incidents from 1997. Hazardous incidents are those situations in the office or the field that present an actual danger, risk, peril, or threat to probation or pretrial officers or assistants during the performance of their official responsibilities, or as a result of that performance. Of the 178 reported incidents, 8 percent involved situations with firearms or edged weapons, 28 percent of the incidents occurred in the office, 56 percent of the incidents occurred in the field, and, in 78 percent of the incidents, the perpetrator was the offender under supervision. As these statistics suggest, the possibility of violence by the offender is prevalent. Consequently, the need to provide officers with adequate training and measures to ensure officer safety is critical.

Many law enforcement agencies, including many probation and/or pretrial offices, are using interactive video training, or a Firearms Training System (FATS), to enhance their officers' ability to win violent clashes or hazardous incidents. In early April 2000, two Missouri Department of Corrections Training Officers, the Firearms Instructor for the Eastern District of Missouri and myself, spent three days training 36 probation officers using an interactive video machine. Nine recently hired officers were trained in teams of two, each team completing 1.5 hours on the FATS machine, while 27 veteran officers were trained in teams of two, each team completing one hour on the FATS machine. Immediately after the training, officers completed an exit evaluation/questionnaire.

The primary purpose of the training was to help officers increase their mental preparedness when faced with a critical incident by presenting realistic, adrenaline-dumping scenarios. However, the training and subsequent exit evaluation/questionnaire were also used to obtain information about the officers' perception of the value of carrying a firearm, the extent the training influenced officers' perception of the probation officer's role, the extent the training changed officers' belief about their ability to use lethal force, the extent the training may affect the officers' performance of field days, and the extent the training had a positive influence on officers' ability to act decisively in a critical situation.

Description of the Training

The FATS machine projects a video image onto a screen or wall, giving the impression of a large television screen. The screen was connected to a computer, two large speakers, and two model 66 Smith and Wesson-like pistols—exact replicas of the pistols which the officers carry while on duty. The officers were required to wear the same clothes and holsters they wear during street work and were provided with an inert cap-stun cannister, which actually sprayed a harmless peppermint concoction when the trigger was pulled. Each scenario was projected on the wall like a life-sized movie, the speakers helping to augment the atmosphere, making one feel as if present in the scenario.

The officers were placed five to10 feet in front of the wall where the images were displayed. They were first required to complete a short session on basic target acquisition, which included a slow-motion replay, in colored lines on the screen, of their barrel location during target acquisition and trigger pull. Thereafter, they were advised the scenarios were about to begin. They were encouraged to use an appropriate level of force on the force continuum, to use good verbal commands, and to consider retreat and cap-stun as options in the situation. Prior to the start of the scenarios, each team of officers was encouraged to enter the situation with a contact and cover officer, and to utilize cover and/or concealment if necessary.

Not only did the scenarios vary between teams of officers, but the outcome of the scenario itself could be altered by the trainers depending on the commands and actions of the officers. A variety of scenarios were used, including the following:

- Officers enter a place of business, meet some police, are unable to exit the business and are eventually confronted by a man with a pistol. The man may open fire on the officers or drop the weapon, depending on the officer's verbal commands.
- Officers approach a home, when suddenly they are confronted by an irate offender with a knife outside the residence. Depending on the officer's verbal commands and actions, the offender may drop the knife, throw the knife at the officers, or drop the knife, pull a gun and shoot at the officers.
- Officers are confronted by an agitated family during a home visit. The offender comes from another room of the house and runs toward the kitchen. Depending

on the officer's actions, the offender may pull a gun from a kitchen cabinet and open fire, or pull a knife and steadily approach the officers waving the knife.

- Officers are confronted by an intoxicated, stumbling man carrying a baby in a car seat as they exit a dwelling. The man blocks the officers' exit. The man may put the baby down, pull a machete, and approach the officers, or he might come at the officers still carrying the baby and waving the machete.
- During a home visit, an individual grabs a resident of the house and starts to choke her and threaten to kill her.

After each scenario, the officers and the trainers discussed or "broke down" the scenario. The officers were asked to justify their actions and consider other options they might have taken. In situations where lethal force was used, the machine replayed the shots and determined which shots would have been disarming or fatal to the offender and/or to bystanders.

Exit Evaluation/Questionnaire Findings

Because of the potential of serious physical harm to probation officers in the performance of their official duties, officers in the Eastern District of Missouri are authorized to carry firearms. Carrying a firearm is optional for all officers in the performance of their duties. All probation officers requesting to carry a firearm are required to attend an initial firearms qualification course, typically consisting of two days of classroom instruction and live firing-range experience under the supervision of certified firearms instructors. Officers who elect to carry a firearm are also encouraged to increase their proficiency in the use of the firearm through practice, primarily by dry firing, shooting at fixed targets, and situational shoot/don't shoot scenarios presented by the firearms instructors at fixed targets. While these training methods can be effective in training officers in basic firearms utilization, safety, and shooting skill, they do not present the officer with realistic, interactive situations that the officer may encounter during the performance of their duties. In short, they are not really effective in developing an officer's mental skill or preparedness. As Charles Remsberg suggests in his book *The Tactical Edge*, "What truly prepared officers can depend on for winning violent clashes is this: mental skill—75 percent, shooting skill —15 percent, physical skill—5 percent, and luck—5 percent."

When officers carry a firearm into any situation, the potential for danger increases merely with the presence of the firearm. Consequently, mental preparation also speaks of another issue: What is an officer willing and capable of doing to survive a critical incident? Is the officer psychologically capable of using lethal force, if needed? If not, should that officer be carrying a firearm and thereby increasing the situation's potential for danger?

For at least eight years, the probation office has provided little realistic scenario-based training incorporating life threatening situations. Because of the lack of training in this area, officers have had few opportunities to develop and evaluate their ability to handle critical situations. For instance, during the initial stages of the training, most of the probation officers exhibited poor verbal commands. They had never been in situations where loud, forceful verbal commands were necessary. While approximately 98 percent of the officers in the Eastern District of Missouri have chosen to carry a firearm, most officers have had little opportunity to experience what it is like to be involved in a critical incident, which can arise in a split second.

METHOD

Each officer was requested to complete an exit evaluation/questionnaire immediately after the training. The exit evaluation/questionnaire was broken into two parts. The first section included the following five questions (see Appendix A):

- After completing the FATS training, to what extent has your perception regarding the value of a firearm for self-defense in the performance of your duties changed?
- To what extent did the training influence your perception regarding your role as a United States Probation Officer?
- To what extent did the training change your belief about your ability to use lethal force within the guidelines of the lethal force policy established by the office and the Judicial Conference?
- To what extent do you expect the training to have an impact on the way you perform your field days?
- To what extent do you believe that the training had a positive influence on your ability to act decisively in a critical situation?

Officers were requested to answer the question by circling the statements that most closely matched their beliefs on the following range of answers:

- to a very little extent
- to a little extent
- to some extent
- to a great extent
- to a very great extent

Officers were also given the opportunity to explain their answers.

The second part of the evaluation/questionnaire included nine questions, primarily designed to evaluate the training and to obtain information to improve this specific training and training in general. These were (see Appendix B):

- To what extent was the overall training effective?
- To what extent were the training objectives clear?
- To what extent were the trainers knowledgeable and prepared?
- To what extent was the training applicable to your duties as a United States Probation Officer?
- What areas of the training should be emphasized more?
- What areas of the training should be deleted from the training?
- To what extent did the training meet your expectations?
- When you return to work, how will you describe the training to your co-worker and/or friends over lunch?
- Please share any comments about the training, or suggestions for future training topics you would like to see.

Of the 36 officers who completed the training, 29 completed and returned the questionnaire, representing an 80 percent return rate.

Interpretation

To what extent officer's perception regarding the value of carrying a firearm had changed since the training?

Since carrying a firearm is optional for all officers in the performance of their duties, the decision to carry a firearm is intensely per-

sonal and one of considerable debate. Officers should contemplate their psychological and physical ability to use lethal force when deciding whether or not to carry a firearm. Firearms training traditionally consists of firing rounds from varying distances at static targets. Although the Eastern District of Missouri Probation Office provides officers with a well-rounded firearms training program that includes the proper use of force on the force continuum and involvement in mock shooting situations, officers rarely have the opportunity to be involved in realistic, stress-filled scenarios where decisions have to be made in a spit second. Consequently, perceptions of the value of carrying a firearm may differ between officers since they rarely find themselves in critical situations. The above question was designed to obtain information regarding officers' perception of carrying a firearm after experiencing realistic, stress-filled scenarios.

Of the questionnaires completed, 28 officers responded to this question, representing a 97 percent response rate. Of those, 18 percent indicated the training changed their perception regarding the value of a firearm for self-defense "to a very little extent," one respondent indicated the training changed their perception regarding the value of a firearm for self-defense "to a little extent," 47 percent indicated the training changed their perception regarding the value of a firearm for self-defense "to some extent," 14 percent indicated the training changed their perception regarding the value of a firearm for self-defense "to a great extent," and 18 percent indicated the training changed their perception regarding the value of a firearm for self-defense "to a very great extent" (see Appendix C).

To get a clear interpretation of the responses to this question, it was necessary to review the written responses to the question in addition to the selected choices. Regardless of choices made on the spectrum, thirteen (46 percent) of the respondents indicated in writing the training reinforced their belief in the need of a firearm for officer safety. One respondent replied, "I have always believed that a firearm is needed for our protection. When you do this type of training, it drives home the risks we take and need for self-defense." Another wrote, "I've always seen the value, but the training drilled it home." Three other respondents were surprised at the speed with which a critical incident can occur, as evidenced by the scenarios, and one respondent wrote "I'd been thinking of giving up the gun, but it reminded me in some situations, only the gun would be effective."

In conclusion, a large percentage of the respondents (66 percent) indicated that their perception of the value of a firearm for self-defense changed at least to some extent because of this training. The responses suggest that officers perceive the firearm as a necessary tool for self-defense and the training, if anything, reinforced this belief. Thirty-two percent of the respondents, however, related that the training changed their perception of the value of a firearm for self-defense to at least a great extent. This is a significant figure. Officer comments generally indicated that officers perceived the firearm as necessary for self-defense, including the 32 percent. It seems reasonable to suggest, therefore, that some officers had a more casual perception of the value of a firearm prior to the training. The training appears to have changed this perception.

To what extent the training influenced officer's perception regarding the probation officer's role?

Professionals who carry firearms are traditionally viewed by the public as law enforcement officers. Therefore, it would seem safe to say that offenders may also view officers who carry a firearm as strictly law enforcement officers. According to our Mission Statement, the Probation Office for the Eastern District of Missouri will complete thorough investigations, provide accurate and timely reports, and provide meaningful supervision services designed to protect the community and promote the rehabilitation of offenders. The role of the probation officer is varied, as the Mission Statement indicates, and "managers convey the authority and the resources each individual needs to do his or her job (Strebel, *Harvard Business Review*: May-June 1996 p. 87)." As indicated previously, the firearm is perceived by officers to be necessary to perform their duties in a safe manner. While adding a firearm for protection may influence how the public and the offender perceive the officer, does it change how officers perceive their own roles? The above question was designed to measure officer perception about their role as probation officers after experiencing life-threatening scenarios.

Of the questionnaires completed, 28 officers responded to this question, representing a 97 percent response rate. Of those responding, 14 percent indicated the training changed their perception of their role as a probation officer "to a very little extent," 14 percent indicated the training changed their perception "to a little extent," 50 percent indicated the training changed their perception "to some extent," 18 percent indicated the training changed their perception "to a great extent," and one respondent chose the answer that training changed their perception of the value of a firearm for self-defense "to a very great extent" (Appendix D).

The firearms policy for the Eastern District of Missouri Probation Office clearly states officers should avoid the use of a firearm except in self-defense or in defense of a fellow probation officer. The officer may not use a firearm unless the officer believes he/she, or a fellow officer, is in imminent danger of death or serious bodily injury and there is no means of a safe retreat. To get a clear interpretation of the responses to this question, it was necessary to review the written responses to the question in addition to the selected choices. Five respondents wrote statements that indicated they had a clear understanding of their role before the training. For instance, one respondent wrote, "unexpected things can happen, so we need to be ready to handle these situations effectively, while maintaining our own safety." Another related the training was "a good reminder of when to back away and when to stay in and be ready," while a third indicated "my role is to avoid these situations, but I have always been aware that things like this could happen."

Although the written firearms policy is clear on when an officer is authorized to use lethal force, it can become less clear when the incident occurs quickly and the officer is under stress. In some scenarios, officers were called upon to act with lethal force outside office policy. The following officer comments support this supposition: "The training was good because it showed how things can go bad quickly and our role can be gray." "Even though we may view our role in a limited way, there may be situations where we are viewed as another law enforcement officer and may need to act beyond the defined scope of our duties." The training "made me realize the differences between our policy and the legal/moral issues regarding lethal force."

In conclusion, the respondent's perception of their role as a probation officer changed very little after the training. Some responses, however, indicate that officers may not have been prepared to handle situations that went "bad quickly." Still other officers appeared dismayed after being placed in a situation where they were viewed by others as strictly

law enforcement officers and had to act accordingly.

To what extent did the training change your belief about your ability to use lethal force within the guidelines of the lethal force policy?

Anytime an officer carries a firearm, the potential for danger increases with the presence of the firearm. Many situations, while dangerous, may never reach the level of immanent danger of serious bodily injury or death when the firearm is not present. But an altercation when a firearm is present becomes much more dangerous. It is essential that any officer who decides to carry a firearm be aware of the increased potential for danger. Officers should have a good understanding about their physical and psychological ability to use their firearms in a critical incident. The above question was designed to measure whether the training affected officers' belief about their ability to use lethal force.

There was a 100 percent response rate to this question among those filling out the questionnaire. Fourteen percent of the respondents indicated the training changed their belief about their ability to use lethal force "to a very little extent," 14 percent indicated the training changed their belief about their ability to use lethal force "to a little extent," 58 percent indicated the training changed their belief about their ability to use lethal force "to some extent," and 14 percent indicated the training changed belief about their ability to use lethal force "to a great extent" (Appendix E).

In traditional firearms training (i.e., firing at fixed targets on command), officers rarely have the opportunity to interact with their subjects. Consequently, officers have little experience in dealing with fluid situations where the outcome may depend on their communication ability and their ability to defend themselves. To get a clear interpretation of the responses to this question, it was necessary to review the written responses to the question in addition to the selected choices. Some responses reflect a concern about the limitation the lethal force policy places on the officer. In many of the scenarios played out during the training, the officers had to decide whether to come to the assistance of a third party. While the firearms policy does not permit the use of lethal force to come to the aid of a third party, some officers felt compelled to do so. One officer indicated that, "I was surprised—I did not always follow policy." Another officer wrote point-blank, "Lethal force policy is *too* restrictive." Most of the officers' responses, however, reflect that the training either confirmed their belief about their capability to use lethal force or improved their ability to make a better lethal-force decision. For instance, one officer indicated that with this type of training, "I become more confident that I will use lethal force if necessary," while another wrote that the training "showed me to always try to leave a threat area whenever possible." Another officer indicated, "It made me realize (believe?) that we have the authority to pull our firearm in response to a lesser force, such as the perceived displaying of a knife (huh!)."

In conclusion, 72 percent of the respondents indicated the training affected their belief about their ability to use lethal force to at least some extent. In fact, some responses suggest the training gave them a better understanding of how complex and restrictive the lethal force policy is and how difficult a lethal-force decision is when made under stress with little time to think. The training clarified the lethal force policy and provided officers with food for thought about the use of lethal force to come to the assistance of a third party.

To what extent do you expect the training to have an impact on the way you perform your field days?

Probation officers often work in the community. As part of their job duties, officers commonly visit offenders in their homes or at their place of employment. As noted in the introduction to this paper, in 1998, 56 percent of the critical incidents that presented an actual danger, risk, peril, or threat to the officer occurred while the officer was in the field. While officers may not necessarily view themselves as strictly law enforcement officers, the offender under their supervision or investigation may have a different view. The above question was designed to measure whether the training affected how officers perform their field work.

There was a 100 percent response rate to this question among those who filled out the questionnaire. Two respondents expected the training to affect how they perform their field work "to a very little extent," one respondent expected the training to affect how he/she performs field work "to a little extent," 31 percent expected the training to affect how they perform their field work "to some extent," 44 percent expected the training to affect their field work performance "to a great extent," and 14 percent indicated the training changed belief about their ability to use lethal force "to a very great extent" (Appendix F).

Officers are encouraged to perform their field work in teams; however, traditional officer training rarely provides officers the opportunity to interact with offenders as well as with each other. To get a clear interpretation of the responses to this question, it was necessary to review the written responses to the question in addition to the selected choices. When working in teams, communication becomes paramount. Most of the officers' responses, in some form or another, suggested that the training showed them the importance of officer communication and the importance of being prepared for a critical incident before it occurs. Some of the written responses were: "I will be more prepared." "Just be as aware as possible." "Lethal problems can arise in a heartbeat." "Will be more careful and always have a backup officer." "I will definitely communicate more with my partner before approaching each home." "The training will make me more aware. It is easy to get relaxed." "I will be more prepared than before, especially to make verbal commands."

As indicated above, officers are discovering and adapting to a new way of operation: the performance of field work in teams and the possibility of stepping outside the defined scope of their role. This calls for new behaviors (i.e., verbal communication) and new approaches to work (Heifetz and Laurie, *Harvard Business Review:* January-February 1997, p. 124).

In conclusion, a majority of the respondents (58 percent) indicated that the training affected the way they will perform their field work at least "to a great extent." The written comments suggest that officers benefitted most from the emphasis on teamwork and communication.

To what extent do you believe that the training had a positive influence on your ability to act decisively in a critical situation?

Officers were presented with a variety of realistic scenarios. All of the situations had the potential to explode, depending on the officers' reactions. After the completion of each scenario, the officer and the trainers analyzed the situation and the reaction of the officers. The use of verbal commands and use of cover and/or concealment were the most common issues discussed after each scenario. In some

instances, the officers would perform the scenario again, often with a different outcome as a result of the "break down." The above question was designed to measure the effectiveness of the training in preparing officers to act decisively in a critical situation.

There was a 100 percent response rate to this question from those filling out the questionnaire. Four respondents indicated the training had a positive influence on their ability to act decisively in a critical situation "to some extent," 62 percent indicated the training had a positive influence on their ability to act decisively in a critical situation "to a great extent," and 24 percent indicated the training had a positive influence on their ability to act decisively in a critical situation "to a very great extent" (Appendix G).

A large majority of the respondents (86 percent) indicated the training had a positive influence on their ability to act decisively in a critical situation. The following written comments support this figure: "It helped to practice acting decisively. We rarely get a chance to do it." "Actually showed me that I can react appropriately." "It (the training) gave me more experience to draw on if I ever find myself in a situation such as these." "Good practice at thinking on your feet—augments our current, ongoing training." "Excellent training to simulate possible real life situations." "It is good to be exposed to a variety of possibilities." "I don't always have faith that my decisions will be good in 'bad' situations. The training was a positive experience." "The training has helped me to feel more confident in my actions regarding self-defense and lethal force." "Requiring us to explain our actions was excellent. It will make us think about our situations more thoroughly."

Both the figures and the officers' comments suggest that the training was effective in influencing officers' ability to act decisively in a critical situation.

Conclusions and Recommendations

According to the evaluations (Appendix H), 97 percent of the officers reported that the overall training was effective to at least "a great extent." Before the training, officers had a certain belief about their ability to perform their job in a safe and effective manner. After the training, officers clearly indicated they were surprised at how quickly a critical incident could occur, how likely it is that they will be perceived as law enforcement officers during a critical incident, how difficult it can be to work in teams and communicate during a critical incident, and how unfamiliar they were in using forceful verbal commands.

This suggests that the training was effective in heightening officer awareness of danger and the necessity for continued training in mental preparedness and self-defense proficiency. It is recommended that an ongoing regime of scenario-based training, including FATS training and other role-play training scenarios, be implemented on at least a semi-annual basis. The training should emphasize working in teams and include a component of communication between officers. It is also recommended that this district explore the feasibility of training officers utilizing scenario-based Simunition training devices.

The training and subsequent data that was collected also indicate that officers have some anxiety over the limitation of the lethal force policy, especially when confronted with a variety of situations involving a threat to a third party. The training did not address this dismay. Future scenario-based training should include a component that seeks information on this issue from officers prior to the training and evaluates the effectiveness of the training in addressing this concern.

The primary criticism of the training related to the nature of some of the scenarios. Since FATS training is typically used by police departments, some of the scenarios were law-enforcement oriented. In future training programs, scenarios designed strictly for probation officers should be used to enhance the training.

Appendix A
Exit Questionnaire/Survey

Program Title: FATS

After completing the FATS training, to what extent has your perception regarding the value of a firearm for self-defense in the performance of your duties changed? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

Please try to explain your answer:

To what extent did the training influence your perception regarding your role as a United States Probation Officer? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

Please try to explain your answer:

To what extent did the training change your belief about your ability to use lethal force within the guidelines of the lethal force policy established by the office and the Judicial Conference? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

Please try to explain your answer:

To what extent do you expect the training to have an impact on the way you perform your field days? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

Please try to explain your answer:

To what extent do you believe that the training had a positive influence on your ability to act decisively in a critical situation? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

Please try to explain your answer:

Appendix B
Training Evaluation

Program Title: FATS

To what extent was the overall training effective? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

To what extent were the training objectives clear? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

To what extent were the trainers knowledgeable and prepared? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

To what extent was the training applicable to your duties as a United States Probation Officer? (Check one)

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

☐ to a very great extent

What areas of the training should be emphasized more?

What areas of the training should be deleted from the training?

To what extent did the training meet your expectations?

☐ to a very little extent

☐ to a little extent

☐ to some extent

☐ to a great extent

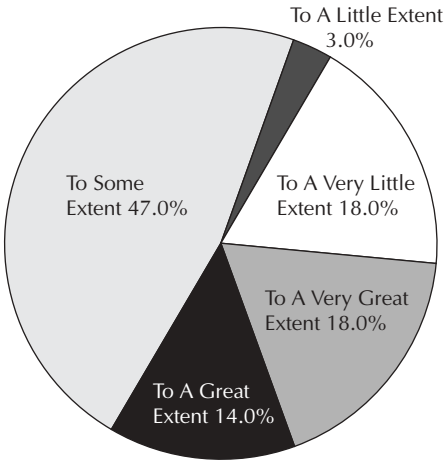
☐ to a very great extent

When you return to work, how will you describe the training to your co-worker and/or friends over lunch?

Please share any comments about the training, or suggestions for future training topics you would like to see.

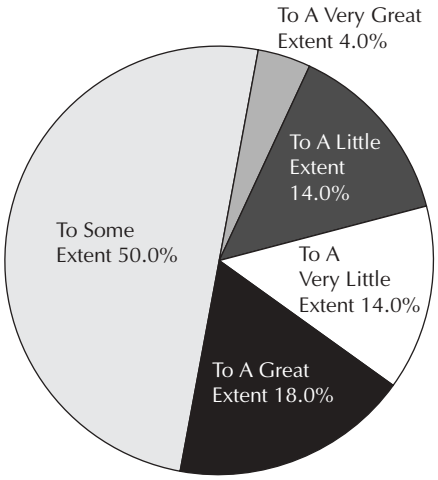
Appendix C
Value of Firearm

To what extent officer's perception regarding the value of carrying a firearm had changed since the training.



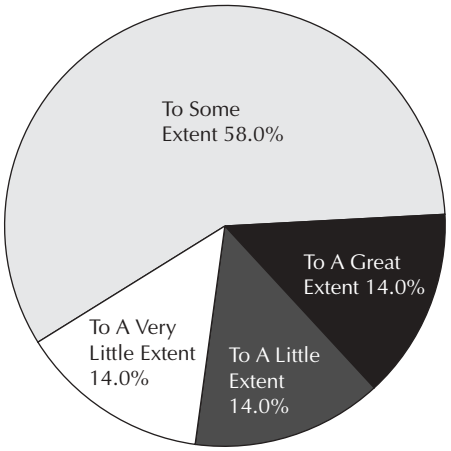
Appendix D
Perception of Role

To what extent the training influenced the officer's perception regarding the probation officer's role.



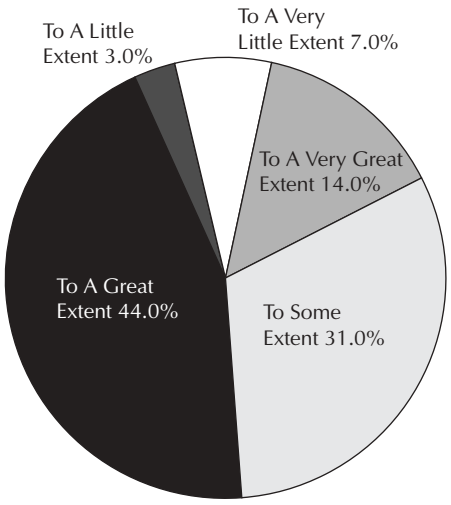
Appendix E
Ability to Use Lethal Force

To what extent did the training change the officer's belief about their ability to use lethal force within the guidelines of the lethal force policy.



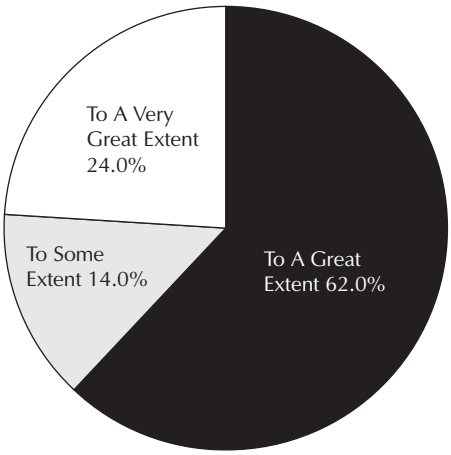
Appendix F
Performance of Field Day

To what extent do you expect the training to have an impact on the way you perform your field days?



Appendix G
Ability to Act Decisively

To what extent do you believe that the training had a positive influence on your ability to act decisively in a critical incident?



Appendix H
Evaluation Results

To what extent was the overall training effective?

to a very little extent	NO RESPONSES
to a little extent	NO RESPONSES
to some extent	1 RESPONSE
to a great extent	38%
to a very great extent	59%

To what extent were the training objectives clear?

to a very little extent	NO RESPONSES
to a little extent	NO RESPONSES
to some extent	14%
to a great extent	45%
to a very great extent	41%

To what extent were the trainers knowledgeable and prepared?

to a very little extent	NO RESPONSES
to a little extent	NO RESPONSES
to some extent	NO RESPONSES
to a great extent	21%
to a very great extent	79%

To what extent was the training applicable to your duties as a United States Probation Officer?

to a very little extent	NO RESPONSES
to a little extent	NO RESPONSES
to some extent	17%
to a great extent	34%
to a very great extent	49%

What areas of the training should be emphasized more?

Thirteen percent of the respondents to this question indicated that the scenarios should be more probation officer orientated. There were no other responses to this question.

What areas of the training should be deleted from the training?

There were no responses to this question.

To what extent did the training meet your expectations?

to a very little extent	NO RESPONSES
to a little extent	NO RESPONSES
to some extent	NO RESPONSES
to a great extent	55%
to a very great extent	45%

When you return to work, how will you describe the training to your co-worker and/or friends over lunch?

A little confusing at first, because we didn't understand our roles in the scenario/Excellent session—very productive—it was very realistic/Excellent (3 responses)/I will tell them it was excellent training, and very beneficial/Fun, interesting, enlightening, educating, humiliating/humbling experience/Very positive and beneficial/A useful training program/Helpful. We could use more of this type of training/It was wonderful and fun/Great, "go have fun and learn"/Worth my time, good practice/It was good/Fun-learned more/A good experience/The scenarios made me realize how quickly a situation can escalate. It was very interesting/Good training. Need to have on a regular basis/Yes-I think any role plays that challenge a person's responses are good and are effective training tools/Very enjoyable/Very realistic, real-life scenarios. The technology enhanced the training, which doesn't always happen/Very good/Worthwhile/Good-makes you think and react quickly/Fun, but makes you prepare mentally for the unknown situations that may occur/Fun

Please share any comments about the training, or suggestions for future training topics you would like to see.

Good to do scenarios—need to continue till I get one right. Maybe could use work on what is presumed obvious, but isn't to all of us—how to tell offender to position himself, commands, communicating with other law enforcement, etc./It would be nice if we could do this training 3 or 4 times a year/Having a cover officer was helpful. There were a lot of scenarios where there was more than one potential threat. If one person had been doing the HV, it would have been more likely that the officer would have been harmed. More training with partners would be helpful/I would like to see us do such training once a year/The training was excellent/I would like to have repeated (at least once) the drill where the machine tracked the gun from leaving the holster, firing and covering the target/We should be doing this type of training on a regular basis/I hope we can do this more often/Great/More of the same type of training/Very appropriate and excellent training/Good training!

Criminal Justice and the IT Revolution

Terence Dunworth
Managing Vice President, Abt Associates

IT WILL NOT BE LONG until personal computers are as common as telephones. This is one consequence of the information technology (IT)[1] revolution that has taken place since the invention of the transistor 50 years ago.[2] Of course, it is now a decade or so since the designation "personal" became inappropriate. What used to be "personal" during the first few years of the revolution has now become general. It is probably not too great a stretch to assert that virtually every organizational, business and scientific use of information incorporates in some way the general IT that is encompassed by the rubric "personal computers." In addition, desktop and laptop systems are moving into public and private organizations, as well as homes, with a rapidity that is far greater than occurred with the telephone, and they seem certain to have (may already have had) a greater impact than the telephone on the way public and private activities are conducted.

The revolution has enormous implications for the criminal justice system, which is generally regarded as a fragmented and sometimes cumbersome processor and user of information.[3] It has provided a capacity for information management that has begun to radically change the way in which law enforcement conducts its business. Though it is true that the pace at which law enforcement has adopted the new IT lags behind many other elements of society, there is also an inevitability about that adoption. In the end, law enforcement will not have a choice. The IT revolution will have to be embraced.

In this article, I have a narrow focus—the effect of the IT revolution on the criminal justice system. This is because criminal justice agencies are, in my opinion, the most dynamic users of the kind of information that the IT revolution is bringing into existence. Criminal justice agencies use information to make strategic, tactical, and investigative decisions in ways that other agencies do not. Criminal justice agencies do a lot more than record their activities, and they are faced with a constant need to adapt to a changing operational environment. In that sense, the IT revolution is a very good fit for their needs.

In the following section, I present a brief historical background of the application of information to law enforcement, beginning with early developments in the nineteenth century and culminating with the 1994 Crime Act.

Following the historical overview, I consider the promise and the reality of information technology for law enforcement, reviewing where law enforcement stands with respect to a number of critical information systems areas: records management; criminal histories and offender identification; the Uniform Crime Reporting System and the National Incident Based Reporting System; and computer networking technology and the Internet.

The final section contains some reflections on criminal justice IT and the 21st century. The potential for the generation of new knowledge and the risks associated with possible misuse of computerized data are briefly reviewed and a short conclusion brings the article to a close.

Historical Background
The First 100 years—1830 to 1930

Though the intensity of our current focus on information systems in criminal justice is historically unparalleled, a demand for facts about crimes, those who commit them, and the response we muster goes back for more than two centuries. In a 1978 article,[4] Decker identified early approaches by Bentham (urging data collection on British prisoners in 1778), Guerry (beginning a formalized system of French criminal statistics in 1833), and Quetelet (who commented at the same time on the issues surrounding the strengths and weaknesses of official French crime data).

Decker noted that in the United States, the effort to develop systematic information about crime dates back about a century and a half. In 1834, Massachusetts was the first state to begin collecting data on crimes. The U.S. federal government did the same, first in conjunction with the 1850 census and subsequently with later censuses. By the early 1900s, data from police reports were being compiled into criminal statistical reports, and federal prisoner data and federal judicial statistics were being accumulated, printed, and disseminated by the office of the U.S. Attorney General.

Though these early efforts were modest by today's standards, the federal systems in particular generated what appear to have been reasonably accurate compilations of the activity of the federal judicial system, and they were used for decision-making about budgeting, facilities construction, and resource al-

An earlier version of this article appeared in NIJ's *Criminal Justice 2000, vol. 3, Policies, Processes, and Decisions of the Criminal Justice System.*

location issues. Data on crime in cities was another matter. Many law enforcement agencies lacked the resources and perhaps the interest needed to compile comprehensive and accurate statistics, and the consequence was that knowledge about non-federal crime and the local criminal justice environment was sketchy, at best.

In the 1920s, the International Association of Chiefs of Police (IACP) responded to the need for a uniform, nationwide system of compiling statistics on crime by developing and initiating a Uniform Crime Reporting System (UCRs), to which police departments were urged to voluntarily contribute crime data in a standardized format. In 1930, IACP cooperated with the federal government in arranging for the transfer of this system to the Federal Bureau of Investigation (FBI), where it is still housed.[5] The 1930 UCR report included 1002 cities, with 83 percent participation of all cities with populations greater than 25,000.

Wickersham Commission, 1931

In 1929, the same year that the UCRs were launched, a National Commission on Law Observance and Enforcement was established by President Hoover. This came to be known as the Wickersham Commission, named after its chair George W. Wickersham.[6] Though there had been locally based studies of criminal justice during the previous ten years,[7] this was the first national evaluation of the system of justice administration in the U.S.

The Commission published 13 reports in June of 1930.[8] One of these, the *Report on Criminal Statistics*, was an assertion of the need for accurate, nationwide statistics on crime and the criminal justice system. The report reflected the influence of the IACP's work on the UCRs, and specifically cited the UCR system as a model. However, the members of the Commission wanted to go much further than the UCRs, by creating a comprehensive system of national data encompassing penal, judicial, and police data under one umbrella federal agency which would establish national data collection systems to achieve these objectives. The report also expressed reservations about the accuracy of the crime statistics currently being compiled, as well as about the interpretations of them that were being made. In this respect, the Commission's observations were prescient—many of its concerns have been repeatedly echoed in subsequent commentary on the UCRs.

Presidential Commission, 1965

For the next three and a half decades, the UCRs were systematically collected and came to be the nation's only barometer of crime levels. However, little progress was made beyond this, except at the federal level, where the creation of the Administrative Office of the U.S. Courts in 1938 consolidated federal judicial and penal system data collection under the new agency and led to the creation of a centralized process of data compilation and reporting that has persisted largely unchanged (except for computerization) to the present time.

Then, in 1965, President Johnson convened the President's Commission on Law Enforcement and Administration of Justice. The mandate of this commission, with respect to issues pertaining to crime, was essentially unlimited, and its extensive report was a wide-ranging and enormously influential document.[9]

The Commission's examination of information systems and statistics produced gloomy observations by commission members. Henry Ruth, deputy director of the Commission, is quoted as saying: "Practically no data on the criminal justice system existed when the Commission began work. Not much police data existed. Court data were a mess."[10] In addition, the Commission's survey of 10,000 households suggested that crime of all kinds was being seriously under-reported to police, with the result that the UCRs could not be counted upon to be an accurate measure of crime levels in the country.[11]

This led to what was in a number of respects a reaffirmation and clarification of the principles and approaches promulgated earlier by the Wickersham Commission, but never adequately adopted. Namely, that policy should be informed by knowledge and facts; that the development, collection, and compilation of these should be the responsibility of a National Criminal Justice Statistics Center; that state statistical centers should be established to both provide information and support to the federal agency and to generate locally useful data; and that federal funding should be provided to help accomplish these goals.

Federal Legislation: 1968–1994

The immediate outcome of the work of the Commission was the passage of the Omnibus Crime Control and Safe Streets Act of 1968, which has been the foundation for virtually all subsequent federal legislation on state and local criminal justice matters.This Act created the Law Enforcement Assistance Administration, which from 1968 until 1979 housed the National Institute of Law Enforcement and Criminal Justice (the precursor agency to today's National Institute of Justice), and the National Criminal Justice Information and Statistics Service (the precursor to today's Bureau of Justice Statistics). LEAA also managed federal assistance to state and local criminal justice agencies,[12] and, in 1973 established the National Crime Survey, which carried forward the approach undertaken by the Commission in the 1967 survey mentioned above. Of the Crime Survey, Tonry notes:

> Some observers would say that the National Crime Victimization Survey is the single most important research-and-statistics legacy of the President's Crime Commission. Considering that there were no victim surveys before the President's Commission sponsored the pilots, the NCVS is a remarkable accomplishment. Not only has it survived for nearly a quarter of a century, and been steadily improved during that period, but it has now achieved recognition as at least equal to the UCR as a source of information on crime trends and patterns.[13]

Despite the promise inherent in the Commission's report and the subsequent legislation, the operational manifestation of the principles the Commission espoused did not generate long-term acceptance by Congress or the criminal justice community. By the late 1970s, the LEAA was an agency whose time had come and gone. Congressional willingness to fund the agency dwindled from the peak reached in 1976, and by 1980, appropriations were effectively zero.[14]

This discontent with LEAA led to an overhaul of the federal government's approach to the management of its efforts to influence and assist state and local crime control activities. In 1979, Congress passed the Justice System Improvement Act of 1979, which took the building blocks created by LEAA and converted them into the federal system for dealing with state and local criminal justice issues that we know today. An independent National Institute of Justice (NIJ) and Bureau of Justice Statistics (BJS) were created within the LEAA framework. An oversight office—the Office of Justice Assistance, Research, and Statistics (OJARS)—was also set up. When LEAA was formally abolished in 1982, the other three offices survived and the Comprehensive Crime Control Act of 1984 created a new structure, retaining NIJ as the research

entity, BJS as the statistics entity, renaming OJARS to the Office of Justice Programs (OJP) with similar oversight responsibilities, and creating two new agencies—the Bureau of Justice Assistance (BJA) to manage block grants and the Office for Victims of Crime (OVC) to handle victim issues. This organizational structure has survived to the present day and most subsequent legislation authorized and appropriated funding within it. The exception was the 1994 Crime Control Act, which, among other things, created an independent agency, the Office of Community Oriented Policing Services (OCOPS) to manage the 100,000 Cops on the Street program of the Clinton administration.

Summary

A common theme about information and statistics can be found in the reports of the two commissions and the legislation that has been enacted. This is that we don't know enough about crime and the criminal justice system, and we must develop more information in order to develop good policy and make sensible operating decisions. Certainly until 1967, this was the clarion call that was being explicitly sounded. Since 1967, various acts have attempted to codify that call into an effective system for gathering, organizing, and disseminating information.

In some respects, these efforts can be considered a success. BJS now produces an impressive array of data series, covering a large variety of criminal justice topics. NIJ sponsors a wide range of empirical research and itself manages a significant data collection effort focusing on drugs and crime.[16] The FBI produces Uniform Crime Reports on a nationwide scale. The National Crime Victimization Survey captures unreported as well as reported crime in ways that most observers consider highly credible and dependable. And at the local level, many police departments have replaced paper records with computerized information systems that would have been infeasible a decade ago.

However, there is a problem. Though the emphasis on collecting facts and increasing our knowledge of the situation with which the criminal justice system must deal is an obvious first step in dealing effectively with crime, data alone cannot tell us what to do. Though it is true that if we don't know the scope of the problem we face, our responses to it are not likely to be appropriately focused, an accumulation of facts is not an answer to policy and operational questions. The facts must be processed in some useful way. They must be analyzed, interpreted, and used as a basis for action. This is where difficulties arise.

Over the past decade or so, extraordinarily rapid increases in data processing capabilities have taken place. What used to take a roomful of hardware to do slowly and sometimes badly can now be done by a machine that we can hold in one hand. We can store vast quantities of records on a device smaller than an envelope. For a few hundred dollars, we can acquire a computing system that is more powerful than one that cost hundreds of thousands twenty years ago. But, in the field of criminal justice, there is a real question facing us: How do we make this new capacity work for us?

By and large, in the operational world, we don't know the answer. Agencies are acquiring capacity without knowing what to do with it, except to automate paper systems. This is fine, but it isn't much of an advance in decision-making.

In the next two sections of this article, this issue will be examined in the context of local law enforcement agencies. In many respects, local law enforcement agencies have the greatest need among criminal justice agencies for a clear understanding of their environment and the ways they can adapt to it. This makes them, potentially at least, the most needy consumers of the new IS/IT that has come on line in recent years. For these reasons they constitute a highly informative context within which to consider the impact of the IT revolution on criminal justice.

Law Enforcement and IT—Promise and Reality

The Promise

This section reviews what has taken place in law enforcement with respect to IS/IT development in a number of important areas during the past three decades. The organizing theme is that the rapid technological advances that have taken place outside law enforcement have promised and sometimes delivered significant improvements in information processing capabilities. It is further believed that the incorporation of these advances into law enforcement operations will at least radically improve and perhaps revolutionize law enforcement. Such advances span virtually all of the information gathering requirements pertaining to crime measurement, control and response that law enforcement agencies might need.

However, despite this promise, the reality in law enforcement has been, and is, quite different. Large-scale data collection systems of crime measurement, such as the National Incident Based Reporting System, have not yet come close to realizing their potential. Few departmentally-based systems have been implemented at anything approaching the level that is technologically feasible. Even when implemented, such systems have often come to be viewed as disappointingly irrelevant to the functions that law enforcement agencies must perform, and a jaundiced view of them is expressed with disturbing frequency by officers and command staff.

The result is that there now exists a real danger that the IS/IT revolution will come to be seen as little more than a faster way of collecting information that used to be put down on paper. If this view prevails, law enforcement will have missed the most important contribution that the IT revolution can make—namely, to assist law enforcement to redefine itself along the lines proposed by community-oriented and problem-solving philosophies.

In the balance of this section, I will present an overview of the status of IT in law enforcement across what I consider to be the most significant substantive areas. These are: Records Management Systems; Criminal Histories and Offender Identification; Crime Analysis; Mobile Data Terminals; Uniform Crime Reporting and the National Incident Based Reporting System; and Computer Networking Technology and The Internet.*

The Reality

The Reality Records Management Systems (RMS)

A Records Management System (RMS) is the informational heart of any law enforcement agency's operations. It provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, and files about every aspect of law enforcement business. A compre-

* I have been assisted in this section by the information contained in a number of presently unpublished working papers prepared by Abt Associates staff members Peter Finn, Kristin Jacoby, Julia Kernochan, Tom Rich, and Shawn Ward. I have made use of the background materials contained in those papers, though the individuals named are not responsible for, and do not necessarily agree with, the interpretations I have made and the conclusions I have drawn.

hensive and fully functioning RMS should include crime and arrest reports, personnel records, criminal records, and crime analysis data. Even today, this is in fact the exception rather than the rule. Though virtually all staff in any law enforcement agency use and depend upon the information that an RMS should contain, many agencies have inadequate or incomplete systems.

Prior to the 1970s, nearly all law enforcement agencies' record-keeping was paper-based. Gradual conversion to main-frame computer record-keeping began in the 1970s, particularly for crime and arrest information, and by the mid-1980s, an estimated 1,500 of the nation's 17,000 law enforcement agencies were using main-frame computers to a limited extent. Characteristically, due to the high investment cost associated with main frames, most agencies shared time with other city agencies and management of the machine and the system was outside the department. Typically the RMS were little more than record-keeping systems, with functions that differed little from those provided by their paper predecessors. As late as 1993, a Bureau of Justice Statistics survey found that only two-thirds of local law enforcement agencies were using computers for some elements of record keeping.[17]

Lack of control over the system, poor links between its elements, and, sometimes, law enforcement agency disinterest in record-keeping or lack of experience and understanding of computers resulted in limited utilization of the RMS that were developed. Even today, many departments have only partial computerization of record-keeping. Some have no automation on key elements of the records system, and a number cannot, for instance, perform simple tasks that computers ought to be able to do easily, such as automatically compile UCR reports, link arrests to crimes reported, and so on. Consequently, in such agencies, these kinds of functions still have to be performed manually, if at all.

More recently, some agencies have begun to move to fully automated (computerized) records management systems. Some of these agencies have gone beyond simply automating record-keeping procedures to implementing dynamic, relational databases as an integral element in information management.

In such agencies, RMS systems are no longer stand-alone systems; they can be interfaced to other systems in the city or county and to State law enforcement systems, which in turn provided access to national crime databases. More recent systems provide graphical user interface with menus, buttons, icons, and other easily recognizable screen images. Built-in editing and error checking can reject incorrect information as it is entered, thus prompting correction before it is stored.

Incident address records are a good example of this capability. When entered by hand, addresses frequently contain mistakes; error rates of 30–40 percent are not uncommon. Now, some agencies have all legitimate city addresses stored in a master file that is scanned whenever an address is entered. Addresses not found are rejected and a prompt for correction is issued. This produces percentage accuracy rates in the high 90s, a critical accomplishment for use with other computer-based applications such as crime mapping.

Thus, state-of-the-art RMS can be integrated with other systems, such as Computer Aided Dispatch (CAD). They can track all the functions of a police precinct, not just arrests and bookings, in one complete package. For example, the latest breed of RMS will manage budgets; keep an active inventory of supplies, property, and evidence; schedule K-9 care and vehicle maintenance; organize intelligence; track 911 data; and automate many other departmental functions.

They also support access to a wide range of external databases, such as the National Crime Information center (NCIC) and National Incident Based Reporting System (NIBRS), and have the ability to share information with other justice agencies at all levels of government.

These capabilities create significant new potential for police departments: to conduct advanced crime analysis; to ground strategic and tactical decision-making on sound information; to determine resource deployment on a pro-active rather than simply a reactive basis; and to execute many other functions that were either impossible to perform under earlier systems or were performed under conditions of extreme uncertainty.

However attractive a picture is drawn, it must be recognized that implementation of an advanced RMS is not a simple matter. Turnkey systems are rarely viewed as attractive by departments considering vendor offerings, and this creates major design issues. Some departments that have committed to state-of-the-art systems spend many months, or even years, in the design phase. Those that do not run the risk of disappointment, disillusionment, and failure. The process takes a major commitment of resources and budget, and can be very difficult to justify to a city council that is already under severe budgetary pressure.

Even when acquired, automated RMS systems require extensive user training, which, because of the expense, departments may neglect or underfund. Officer resistance can also be a factor, because the modern RMS imposes information collection demands on officers that many view as at best irrelevant and at worst obstructive. Agencies must normally consider hiring new staff or training in-house staff to provide ongoing user training and support, as well as system maintenance and troubleshooting. Historically, police departments have not attempted to hire such staff.

Another common concern addresses liability and security with respect to personnel files and other sensitive data such as investigation reports and criminal files. As computer-based applications have grown, so have security breaches. Even government systems that are protected by the most sophisticated national security systems have yielded to persistent hackers. When a major objective of computerization is to simplify the exchange of information among and between officers and headquarters, the risk of improper access is obvious.

Despite these caveats, it is evident that no department will be able to take full advantage of the benefits that the IT revolution offers if it does not acquire a modern RMS. In a real sense, all other IT applications depend upon the RMS. If it is absent or deficient, then a domino effect seems inevitable. The other applications will either not realize their potential, or they will fail outright.

Criminal Histories and Offender Identification

As noted above, a critical component of record-keeping involves criminal histories and offender identification. These have always been problematic areas for police departments. There are two main reasons for this. First, definitive identification at the time of arrest is sometimes difficult to achieve. Some arrestees simply give false names and carry no documents. The result is that a delay in identification occurs and police records are, for a period of time that in some cases can be lengthy, inaccurate or incomplete. Second, even when identification is made at the local level, linking the offender to his/her records in other jurisdictions can be a difficult and tedious process. Since arraignments usually

have to be held within 48 hours of arrest, this can lead to bail decisions that would be quite different if the full history were known.

These problems were first widely discussed in 1967, with publication of the report by the President's Commission on Law Enforcement and the Administration of Justice, which noted that criminal history records were frequently inaccurate, incomplete, and inaccessible. These problems persist. A data quality survey conducted in 1997 found that only 25 of the 50 states surveyed reported that 70 percent or more of arrests from the past five years in their criminal history database had entries for final dispositions.[18]

What is obviously needed are identification and history systems that overcome these problems quickly and efficiently. Ideally, these should be integrated into the RMS. Computerization offers that potential, though it would be accurate to say that the potential has not yet been realized.

Nevertheless, both federal and state criminal history and identification systems have evolved significantly over the past few decades. States have established criminal history repositories that contain information about arrests occurring throughout their state. The FBI maintains criminal history systems for federal offenders and a national criminal records systems, including the National Crime Information Center (NCIC) and the Interstate Identification Index (III).

Initially, most states maintained something akin to a manual index card system that contained a list of arrested persons, perhaps with accompanying paper folders that contain documentation about individual arrests. Over time, most states have automated these files to some extent. Individual law enforcement agencies can query them via remote terminals. At the national level, the FBI is currently moving towards an automated National Fingerprint File (NFF).

Over the past decade, the federal government has invested more than $200 million to improve the quality of criminal history records at state and federal levels. These records are not only critical to the day-to-day operation of virtually every federal, state, and local criminal justice agency. They are also of increasing relevance to non-criminal justice applications. Most states permit some access to criminal history records by agencies outside criminal justice for employment, licensing, and other purposes.

Perhaps of greater significance are the mandates imposed by the Brady Act and the National Child Protection Act of 1993.[19] These significantly expanded the importance of criminal history records for determining eligibility to purchase a firearm and for screening childcare facility employees. Though there is a good deal of controversy about the constitutionality and efficacy of this process, some evidence exists that it has had an effect. The Bureau of Justice Statistics has reported that from March 1, 1994 to November 29, 1998, approximately 12,740,000 applications for handgun purchases were made. There were 312,000 rejections as a result of the background checks required by the Brady law.[20] Whether this should be considered many or few may be a matter of debate. What is not at issue is the dependency of this result on automated information processing that could not even have been attempted a decade ago. Like it or not, the ability to perform such checks is a remarkable IT achievement.

Expansion of such checking seems assured for the future, and, given the expanding public and political attention being paid to gun violence, there seems no doubt that the checks considered necessary will become increasingly demanding and sophisticated. Anyone who has examined the amount and type of information generated by a single arrest knows that it can be complex and voluminous, perhaps involving several agencies within a single jurisdiction. Compiling a comprehensive criminal history involves multiple jurisdictions. In order to have complete, accurate, and timely access to such histories, each step in the process must be carefully executed, and the results must be subject to the most rigorous quality control.

To achieve these goals, federal, and state agencies will need to implement a number of different strategies. These will include: baseline audits of record systems to understand the nature and extent of data quality problems; entering backlogs of manual arrest and disposition records into automated files; developing long-term data quality improvement plans; and undertaking efforts to obtain unreported dispositions from courts and prosecutors. To date, this has been a Sisyphian task due to the fact that much of the desired information exists only on paper or, even if automated, in non-standardized form. Consequently implementing dependable and uniform electronic interfaces between reporting agencies and the central criminal history repository will be a prerequisite for expansion in the effective utilization of criminal histories. In fact, a good deal of work is being done to bring this about.

The Bureau of Justice Statistics (BJS) currently manages a major federal initiative—the National Criminal History Improvement Program (NCHIP)—that provides funding to the FBI and state criminal history repositories. The goal of the NCHIP program is to ensure that accurate records are available for use in law enforcement, including sex offender registry requirements, and to permit states to identify ineligible firearm purchasers, persons ineligible to hold positions involving children, the elderly, or the disabled, and persons subject to protective orders or wanted, arrested, or convicted of stalking and/or domestic violence. NCHIP also provides funding to the FBI to operate the National Instant Criminal Background Check System (established pursuant to the permanent provision of the Brady Handgun Violence Prevention Act), the National Sex Offender Registry (NSOR), and the National Protective Order File.

These developments move law enforcement closer to the goal of rapid identification and accurate recovery of history information. The key, in the end, will be the extent to which individual criminal justice agencies develop the capacity to take advantage of the state and federal systems that are being created. This is another of the IT challenges that criminal justice agencies face.

Mobile Data Terminals (MDTs)

During the past decade, another important element of law enforcement response capability has been developed through Mobile Data Terminals (MDTs). These allow wireless receipt and transmission of information to and from officers on foot or in patrol cars. Initially, MDTs were basically unsophisticated terminals that permitted transfer of rudimentary information between station and officer. Dispatch instructions, for instance, could be sent to the terminal rather than being put out over radio. Officers could automatically record and transmit arrival times at the dispatch location. In the past few years, however, technological advances have led to the introduction of laptop and notebook computers, pen-based computers, voice-based computers, and hand-held ticket issuing computers. These now match desktop machines in sophistication, and, in the future, will continue to expand in capability. As miniaturization progresses, for instance, hand-held devices that do not require patrol car installation seem certain to proliferate. This will free officers

from patrol car dependence, and increase the scope and sophistication that officers on the street can exercise with respect to two-way information flow. In this sense, MDTs are becoming much more than aids to response.

First available around 1990, today's laptop models can be operated by officers on a standalone basis or combined with on-board radios, built-in cellular phones, or computer docking stations. In terms of technical capacity, law enforcement laptops equal any other machine. One difference is construction—enforcement laptops tend to be "ruggedized" to withstand the shocks and rough handling that a law enforcement environment potentially inflicts. When connected to cellular phone-based systems, laptops can send and receive data to and from remote sites. Some laptop computers provide touch screen capability. The potential utility of these machines is obviously vast. Not only can virtually any kind of information be transmitted back and forth, they can be used to provide rapid authorization for law enforcement actions through faxed warrant requests and approvals, thus eliminating the sometimes crippling delays that, in the past, could result from having to return to the station, write up a justification, submit it, and then return to the scene.

Hand-held ticket issuing computers, used principally in parking enforcement, enable officers to issue computer-generated citations and simultaneously check the vehicle for outstanding tickets. These systems, which contain as many as 40,000 records, including information on stolen or wanted vehicles, and can also be used to record field interviews.

Pen-based computers, first introduced in 1989, are clipboard-size mobile computers, weighing less than five pounds, that recognize handwriting and convert it to text. Some pen-based computers have radio capability. Pen-based computers can be mounted in patrol cars, but officers can remove and operate them for a limited distance from the vehicles. Because the software used to recognize handwriting was initially perceived as inflexible, pen-based computers have not gained large-scale acceptance in law enforcement. This is certain to change as departments see the benefits of the technology that is now common in business use of hand-held devices. (Gapay 1992)

Computers that offer voice recognition and translation for input to computer files are in a similar category to pen-based systems. Rapid improvements in technology are making such devices much easier to use—by 1996, voice dictation technology was already 95 percent accurate at a dictation rate of over 70 words per minute. The disadvantage is that the technology still requires considerable user (and machine) training. This burden declines each year, and is going to decline more as the technology gets better. Accurate computer "listening" to normal human speech will become generally available within the next few years. Given the obvious advantages of effective voice input over pen or keyboard, the use of voice recognition seems likely to be the next MDT advance. This promises a very significant reduction in the amount of officer and headquarters staff time that is presently consumed by the reporting function.

Though there are few empirical studies of the impacts of MDTs, their reported benefits include:

- speed of information dissemination
- saving officers time and effort
- facilitating information sharing
- increasing reporting accuracy and uniformity
- enhancing response time
- increased officer safety

There are, however, some considerable obstacles to implementation of MDTs. These include expense, a lack of information about available products, a need for significant amounts of user training, and possible officer resistance to or misuse of the devices. All of these seem likely to decline in importance as progress continues, but their short-term effect has been to limit the implementation of MDTs in the policing world.

For example, a 1995 Police Executive Research Forum (PERF) survey of 210 departments drawn in part from among 1995 COPS MORE federal grant recipients found that only a small percentage of police departments had MDTs in patrol cars.[21] However, within that minority, many departments had been using laptops in patrol cars for years.

In 1997, the National Institute of Justice sponsored a study by the National Law Enforcement and Corrections Technology Center on the ability of different agencies to communicate across jurisdictions with each other (so-called "interoperability"). A total of 1,344 agencies responded to the questionnaire. The agencies that were currently using MDTs employed them primarily for database information and free text (e.g., reports, queries). Nearly one quarter of the agencies (24 percent) used database information (primarily agencies with 500 or more sworn officers), and 21 percent of all agencies used free text. However, the use of MTDs was far less common in smaller agencies–as low as 4 percent of agencies that employed fewer than 10 sworn officers.

Despite current limitations, more departments can be expected to use MDTs. Some federal funds are being provided to assist purchase. An added impetus for implementation is to enable officers on the street to take advantage of the FBI's new National Crime Information Center (NCIC) 2000 and Integrated Automated Fingerprinting Identification System (IAFIS) initiatives. MDTs will also assist departments to conform to the new incident-based reporting standards of the National Incident Based Reporting System (NIBRS). These clear advantages, coupled with declining cost and increasing ease of use, suggest that it will not be long until virtually every department uses MDTs of one type or another.

Crime Analysis

The International Association of Crime Analysts (I.A.C.A.) offers this statement about crime analysis:

> Crime analysis is a scientific process in the sense that it involves the collection of valid and reliable data, employs systematic techniques of analysis, and seeks to determine, for predictive purposes, the frequency with which events occur and the extent to which they are associated with other events.

In more concrete terms, Reuland identifies four specific functions for crime analysis:[22]

1) *To support resource deployment.* Crime analysis for this purpose involves detecting patterns in crime or the potential for crime in order to enhance the effectiveness of daily patrol operations, surveillance, stakeouts, and other tactics. These analyses influence personnel deployment and resource allocation.

2) *To assist in investigating and apprehending offenders.* By comparing files that contain *modus operandi* characteristics with files of new suspect attributes, departments hope to make more and better arrests.

3) *To prevent crime.* Crime analysts focus on identifying locations, times of day, or situations where crimes appear to cluster so that departments can take steps to

"harden" these potential targets to make them less likely targets of crime.

4) *To meet administrative needs.* Law enforcement administrators need to provide other individuals and agencies with crime-related information, including city agencies, courts, government offices, community groups, and the media. Administrators may need to use crime analysis in this context for legislative, political, and financial purposes.

Crime analysis may also serve strategic purposes for planning agencies, crime prevention units, patrol and investigative commanders, and community relations units in terms of their programmatic, planning, development, and evaluation functions.

It is clear that crime analysis is a process for which computerized data processing is tailor made. However, it is true that law enforcement agencies have been doing some form of crime analysis from time immemorial. Policing hasn't been random and it hasn't been reactive to the exclusion of all other considerations. Crime analysis has always guided decision-making. However, the crime analysis that we think of now is orders of magnitude different from what was performed prior to the advent of desktop computers. These have increased the power and speed of crime analysis tremendously. The advent of community policing has provided another recent impetus to enhanced crime analysis. For these and other reasons, the number of departments with crime analysis units has been growing over the past several years.

The five stages of crime analysis illustrate the natural fit with the IT revolution:

1) *Data collection.* Law enforcement data are generated primarily from records and reports within the department. Data sources internal to the department include field interviews, offense reports, investigative reports, arrest reports, evidence technician reports, criminal history records, offender interviews, traffic citations, intelligence reports, and calls-for-service data. For community policing purposes, information is also likely to come from non-police sources, such as schools, utility companies, city planners, parks departments, social service agencies, courts, probation and parole agencies, other police agencies, and the Bureau of the Census (e.g., for demographics of a given area).

2) *Data collation.* Departments create databases capable of automated searches and comparisons. Basic database requirements include completeness, reliability, and timeliness.

3) *Analysis.* Departments analyze crime data to detect patterns of activity that can predict future crimes. Crime mapping has become an increasingly popular analysis approach (see below).

4) *Dissemination.* Departments prepare data for internal and external users. Face-to-face contact between crime analysts and officers and investigators, and with some other users, can be important for developing a mutual understanding of the data and their usability.

5) *Feedback.* Measuring users' satisfaction with the information they are given is essential. Crime analysts need to find out what products and formats work and do not work. They must also learn how end users plan to use their products. Analysts can use a simple, closed-ended survey form to obtain feedback, as well as personal contact.

The most prominent crime analysis technique to have been developed as a direct consequence of the IT revolution is computerized mapping. Although computers have been used to display and manipulate maps since the 1960s, the use of mapping software in criminal justice is a relatively new phenomenon. Its growth is due largely to the recent development of inexpensive yet effective and sophisticated PC-based mapping software packages and to the emphasis being placed upon it by the federal government.[23] The application of mapping software to urban settings depends upon the existence of addresses in the data being mapped. Consequently, mapping is most likely to be used for crime analysis in medium and large police departments where computerized address data are a by-product of routine, day-to-day work.[24]

However, utilization is by no means universal. In 1994, 30 percent of 280 member departments of the International Association of Chiefs of Police Law Enforcement Management Information Section (among the most active users of computer technology among local departments in the nation) reported having used mapping software. A 15-month survey of 2,000 law enforcement agencies conducted by the National Institute of Justice Crime Mapping Research Center found that 261 used any computerized crime mapping. Not surprisingly, larger departments (more than 100 sworn officers) were much more likely to use the technology (36 percent) than were smaller departments (3 percent).[25]

Despite the widespread availability of computers and the growth of applications software that seems to closely fit policing's crime analysis needs, the majority of police departments have not yet embraced a comprehensive approach to crime analysis.[26] A number of obstacles that inhibit a commitment to crime analysis can be identified:

- the perception by some sworn officers that crime analysis is not real policing and contributes little to understanding the street conditions under which they have to work;
- the fact that crime analysis is often conducted by civilians, who lack the standing within the department to promulgate the results of their work and its implications for strategic and tactical decision-making;
- uncertainty regarding hardware and software technology, and the difficulty of mastering the range of available techniques;
- inaccurate or missing data in police records systems (e.g. addresses for mapping applications);
- difficulty making arrangements to obtain necessary data from other agencies;
- inadequate or non-existent crime analysis training; and
- insufficient funding.

The principal obstacles to more agencies conducting better crime analysis seem likely to decline as hardware, software, and data acquisition costs decline, as user expertise increases, and as data quality improves. Nevertheless, many departments are still some distance away from the acceptance of crime analysis as an important policing tool.

Uniform Crime Reporting/ National Incident-Based Reporting System

The discussions so far have focused primarily on IT as it relates to individual departments. However, critical needs exist with respect to aggregate measures of reported criminal activity and documentation of national crime trends. These needs have historically been addressed by the Uniform Crime Reporting (UCR) system, which began operation in the early 1930s and has been in place with little change ever since. The system is

dependent upon local police departments, which voluntarily submit a variety of aggregate data to the FBI each year in standardized format. Compilations of UCR data, published annually by the U.S. Department of Justice under the title *Crime in the United States*, generate a statistical overview of data about law enforcement administration, operations, and management, and have served as a primary source of information for researchers and the public. *Crime in the United States* offers sections on the UCR's major topics: crimes cleared, persons arrested, law enforcement personnel, and a Crime Index based on 8 selected offences. However, the UCR system is unable to link an offense to its associated arrest, and the system is believed to have a number of significant limitations.

Because of these perceptions, it was acknowledged in the mid-1970s that a revised and enhanced UCR system was needed for use into the 21st century. This coincided with advances in information technology that made a more sophisticated system feasible. The Bureau of Justice Statistics and the FBI funded a substantial examination and reassessment of the UCR program which culminated in the 1985 publication of a *Blueprint for the Future of the Uniform Crime Reporting System.*[27]

The *Blueprint* proposed the National Incident Based Reporting System (NIBRS) to replace the existing UCR system. The plan called for incident-based reporting, rather than aggregate reporting, represented by two levels of reporting complexity, the more detailed of which would be followed by only 3 percent to 7 percent of law enforcement agencies nationwide. Ultimately, the law enforcement community endorsed the NIBRS framework but elected to institute the more complex reporting level for all participating agencies.

To achieve standardization across jurisdictions, the FBI sponsored the development of new offense definitions and data elements for the new system. Based on the results of a pilot program at the South Carolina Law Enforcement Division (SLED), representatives of the law enforcement community in 1988 approved the revised UCR guidelines and voiced overwhelming support for the new system.

Representing both an expansion of UCR and a major conceptual shift, NIBRS is an "incident-based" system that collects detailed information on individual crimes, including data on location, property, weapons, victims, offenders, arrestees, and law enforcement officers injured or killed. In addition, under NIBRS the scope of reporting is widened to cover 22 crime categories that include a total of 46 specific offenses, known as "Group A" offenses. For an additional 11 "Group B" offenses, NIBRS collects detailed data on persons arrested.

Whereas UCR requires local law enforcement agencies to report monthly aggregate figures on crimes and arrests, NIBRS asks local agencies to submit data on individual incidents for compilation at the state and federal levels. This offers a potential for analysis that would be impossible using only the UCR aggregates, but it also decreases local agencies' control over dissemination of information.

Despite the potential benefits of NIBRS to law enforcement management, training, and planning, law enforcement agencies have been relatively slow to adopt the system. As of May 1997, only 10 states were certified to report NIBRS data, and only 4 percent of U.S. criminal incidents were reported under NIBRS. Large law enforcement agencies have been especially reluctant to make the transition to NIBRS: as of May 1999, the Austin (Texas) Police Department remained the only agency serving a population over 500,000 to report NIBRS data.

According to a recent SEARCH study, law enforcement agencies see lack of funding as the primary obstacle to full adoption of NIBRS.[28] Indeed, the costs associated with the transition can be substantial, especially as many law enforcement agencies have existing records management systems that are either too antiquated to function effectively or are incompatible with NIBRS requirements.

The study also indicated that local law enforcement decision-makers remain unsure of the benefits of NIBRS reporting, and perceive several possible drawbacks to the new system. Although the greater accuracy offered by NIBRS is desirable in principle, some local officials fear a negative public reaction in the event that more precise reporting gives the impression of rising crime rates. Moreover, many officials view NIBRS as a tool for academic research rather than daily law enforcement, or are concerned that reporting the more detailed information requested by NIBRS will place an undue burden on officers in the field. Study participants also discussed the need for federal agencies to encourage participation in NIBRS by reaffirming their commitment to the program and providing better education as to the aims and utility of the revised system.

Of course, the technical and cost problems are not created by NIBRS information needs. They are a consequence of the outmoded and inadequate IT systems that many departments have in place. In fact, as departments upgrade and automate record-keeping systems, they do generate computerized data that would meet all of NIBRS needs, provided the requirement for cross-jurisdictional standardization of definition of offenses and other data elements can be achieved. Most big city departments, for instance, now have data systems that contain a good deal more than the NIBRS date elements and some perform analyses that match in sophistication those contemplated by NIBRS advocates. This suggests that the main obstacles to more widespread implementation of NIBRS are not so much technical or financial, but rather derive from perceptions that it contributes little to local needs for crime analysis and information, while simultaneously containing a good deal of risk to local jurisdictions. In this sense, the potential contribution of NIBRS seems destined to be greatest at regional, state, and national levels. It remains to be seen whether the perceived value of this potential will be sufficient to mobilize the voluntary local commitment to participate upon which NIBRS depends.[29]

Computer Networking Technology and the Internet

The topical reviews provided earlier in this section demonstrate that advances in information technology, combined with law enforcement agencies' increasing emphasis on crime prevention, community policing, and problem solving, is redefining the pursuit and use of criminal justice information. The development of incident-based reporting systems and increasingly sophisticated techniques of crime analysis have caused sharp increases in the volume and complexity of collected data. As this has occurred, new technologies have begun to play a crucial role in agencies' efforts to disseminate, share, and manage this torrent of criminal justice information.

Within the last ten years in particular, computer networking–linking two or more computers so that they can share information—has revolutionized the way we exchange and access data. Many organizations use internal networks, or intranets, to connect the computers within that organization. When two or more individual networks are connected, an internet is formed. The most advanced public level of such systems is of course the Internet, a vast collection of interconnected computer networks worldwide,

serving over 35 million users per year.[30] The easy-to-use World Wide Web (known simply as the Web) is the most popular area of the Internet, and consists of "sites" dedicated to various topics.

This rapidly evolving technology has created a host of challenges for law enforcement officials, whose previously disconnected agencies seem especially suited to benefit from networking technology. Networking centralizes data in order to streamline administration and help agencies collect and manage huge volumes of crime-related information. Additionally, computer networking plays a valuable and expanding role in facilitating communication at all levels: among the local, state and federal agencies; between local agencies and constituent communities; or across agencies within a given region or locality.

One of the Web's most common law enforcement applications has been the establishment of web sites to facilitate communication with the communities served. As of August 1997, over 500 local law enforcement agencies maintained web sites, and the establishment and expansion of sites continues at a rapid pace.[31] Information on the Web is presented in a lively and interactive format, and may be accessed by interested persons at any time from anywhere in the world. By allowing agencies to interact cheaply and easily with members of their constituent communities, an effective Web site can significantly enhance police-community relations and further community policing objectives. In responding to a faxback survey by the FBI, for example, most departments that have sites on the web reported extensive use and positive responses from citizens.[32]

Web sites can fulfill multiple functions for law enforcement agencies. Most sites disseminate a range of public safety information, including: self-protection tips; crime reports and advisories; news of recovered stolen property and local fugitives; clarifications of laws and answers to frequently-asked questions; statistics and budgetary information; community announcements; and information about the agency and its staff. On some sites, communication is two-way, allowing the public to interact with the agency that serves them. Citizens can use the web to apply for permits, file reports on minor incidents, offer tips and information on crimes, and respond to the agency's performance. A web site makes it more likely that community members will contribute to the agency's work, since it is easier and quicker to use the Internet than to go to the agency's office. Web sites can also reduce recruiting costs for agencies, who are able to widen their pool of applicants and provide prospective employees with information.

The equipment required to establish a web site and make quite sophisticated offerings is simple and relatively inexpensive: a computer, a word processing program, a Web processing application, and, for some applications a digital camera and a scanner. Personnel resources may be harder to come by, but a small industry of experts now exists and assistance is easy to obtain. As Internet use has spread among law enforcement agencies, web design companies have developed expertise in creating law enforcement sites, and many Internet service providers have begun to donate access and expertise to local police and sheriff departments.[33] Departments have found web sites to be very cost-effective; once the site is set up, the cost of maintenance is minimal, and sites reduce expenditures for publishing public records and recruiting employees.[34]

However, the Internet is not a panacea. Law enforcement agencies that use web sites to connect to the community must be aware that not all residents use or have access to the Internet. There is an access bias, because low-income residents are less likely to be familiar with and have access to the Internet than affluent residents in the same area. Some will not have computers; others will not even have telephones. Thus, agencies should continue to pursue traditional methods of public education, such as posters or meetings, in order to reach everyone in the community.

A potentially valuable application of networking technology could lead to integrated justice information systems. These are essentially computer internets that would link numerous separate agencies—police departments, prosecutors, courts, etc. Integration may also be pursued among different levels of government, within geographic regions, and/or across disciplines. The cited benefits of integrated justice information systems are clear: they improve the quality of data available to all users; save time and money by eliminating redundant data entry; facilitate timely access to information; and permit accurate information sharing across distance and time. For many years, the fragmentation and lack of coordination among criminal justice agencies has been deplored; the criminal justice system, according to many, is not a system. Networking seems to offer the potential for addressing this problem.

Setting up an integrated system typically demands an extended planning process, requiring the participation of all stakeholders. The planning process involves building support for the project, needs assessment and strategic planning for the project, setting standards for data collection, identifying technological solutions and establishing an oversight board for acquisitions and implementation. During the planning phases, particular attention must be given to setting information systems standards, which have been called "the linchpin to integration."[35] For successful integration, standardization is required in several areas: data definitions; a common language for use between information systems; communications protocols used between agencies; procedures for transferring different types of information (e.g. photos, fingerprints); and security.

The foregoing indicated that regardless of the advantages of integration, it should not be undertaken lightly. Rather, it is an extended process that requires substantial financial and human resources, as well as a sustained commitment from all involved agencies, to be completed successfully. A qualitative study conducted by SEARCH indicated the following primary obstacles to adoption of integrated justice information systems:

- Persistence of entrenched information processing systems and data at local agencies.
- Difficulty of coordinating interagency projects.
- Limited understanding of technological issues and capabilities.
- Need for systems to be private and secure.
- Fundamental inter-agency differences in recording/reporting systems.
- Shortage of information technology professionals.

Though the impediments to establishing integrated justice information systems are significant, a number of evaluations strongly suggest that the benefits of integration are worth the effort.[36]

Outlook for the 21st Century

To characterize the IT developments of the past 50 years as a revolution is no overstatement, in my view. The changes in information technology that have taken place *are* revolutionizing our lives. And, even more rapid change is surely at hand. For the foreseeable future, we can expect the pace of IT

innovation and development to continue to be extraordinarily rapid. This will be particularly noticeable within what can be thought of as the current IT paradigm. For instance, further miniaturization and increased speed of components will likely characterize most advances. Memory and storage capacity of machines will increase even as the machines themselves shrink in size. As long as monopolistic or oligopolistic conditions do not prevail, the unit cost of these developments will continue to fall as installations proliferate. We are able to do now what was prohibitively expensive ten years ago. In the early 21st century, it will be possible to routinely do for a few hundred dollars what is technically or financially infeasible now.

Though, as I have tried to illustrate in this article, the criminal justice world is not at the forefront of the revolution (and probably shouldn't be), it is nevertheless moving inexorably in the same direction. The IT revolution is bringing change in the system's way of doing business that cannot be avoided. I would argue that it shouldn't be avoided, because, properly managed, the change can be beneficial. But, as criminal justice agencies make these changes, there will be side effects. Some of these will probably also be beneficial; but some bring risk.

In this final section, I will first summarize in very general terms what I think criminal justice agencies—law enforcement agencies in particular—will face. I will then briefly review two likely side effects, one almost certainly positive, one possibly negative. The former is the probable advancement in policy-relevant knowledge that can be derived from the expanded information that agencies will have available. The latter is the risk of misuse of the information, and the invasion of privacy that might ensue.

The Information Future for Criminal Justice Agencies

In the 21st century, officers on the street, or in their cars, will have instantly available at the touch of a button more information than can presently be mustered in most agencies. For example, wireless transmission of images as well as text or data will become commonplace. Maps, scene diagrams, photographs, paintings, sketches, fingerprints—all will move back and forth effortlessly. Handheld DNA scanners are being predicted within ten years.[37] On the spot DNA checks will become possible, through wireless transmission of the scanner's reading and an instantaneous comparison with millions of DNA records in a central data bank.

The major question for criminal justice agencies will not be whether information at this level of sophistication is going to be available. The question will be whether it can be used effectively.

For this to happen in a way that is helpful and useful, agencies will have to change. The way things are done will have to be different. New kinds of information will have to be processed and incorporated into strategy and tactics. Officer training will require redefinition and reorientation.

Of course, the basics of law enforcement will have to be retained. A significant portion of future criminal activity will have characteristics similar to criminal activity of the past. A robbery will still involve a robber and a victim, and officers will still need to respond to calls for service, especially emergency calls, in the way they always have. In this sense, the criminal justice system will need to retain the traditional elements of its business, while adding new approaches and techniques that at present are either non-existent or are in their infancy.

The impediments to successfully implementing IT solutions are very substantial. Significant investments of resources, time, and money will all be required, and, perhaps most important, agencies will have to change. In some senses, several Catch-22 problems must be resolved.

For one thing, it is difficult to see the benefits of the new IT until it is in place and operational. But it will never be in place and operational if agencies do not accept its benefits on faith, because the path outlined above is very difficult to successfully implement on a piecemeal basis. This makes it highly desirable for the federal government to promote the incorporation of new technology into departmental operations through any means that are available—financial support, training and technical assistance, widespread dissemination and promulgation of the benefits of advanced IT, conferences, and so on.[38]

There is another Catch-22 in the interplay between design and cost. It is well known that development and design issues are difficult and expensive to overcome. It is not uncommon to see agencies struggle with the design issues surrounding automation for a number of years. It is also easy to find agencies that have had significant problems with vendors who proved unable to deliver the system that was promised. Given this, it is perhaps not realistic to expect agencies to accept turnkey systems. There will be an inevitable desire to tailor new systems to idiosyncratic requirements and standards. The result would be a series of one-of-a-kind systems, which would constitute an astronomically expensive IT trajectory for criminal justice as a whole, as well as for individual agencies. Yet there is a powerful belief in most agencies that their situation is unique. It will be difficult to reconcile these two tendencies.

Another problem exists with respect to officer training and capabilities. What do we want an officer to be? It was already noted above that the response capability that is loosely defined as "traditional" needs to be retained. Can the officer who does that well also be the officer who processes and uses the new kind of information that is going to be available? The answer to this question is not clear. For instance, being comfortable using or even perhaps writing a Visual Basic program to tease out the nuances of crime patterns in a precinct is not going to seem very pertinent to an officer confronting an armed burglar in a dark alley. The question is: shall we, should we, expect an officer to take care of both of these kinds of tasks? Is that a desirable goal? A feasible goal? Does this require an officer for all seasons, and is such an officer available? That is a matter for careful debate that is beyond the scope of this article, but is something that must be addressed.

However, if these and probably other issues that I haven't touched on or thought about are resolved, then the biggest remaining problem facing criminal justice agencies as IT advances is effective utilization. A comparison can be drawn to automated word processing, which, so far, is probably the most frequently used aspect of the IT revolution. Sophisticated word processing software is now provided free with many PC purchases, and, if not free, can be obtained at relatively low initial cost. But, many users are able to employ only small portions of the word processing capability that is accessible to them. The instruction manuals are inches thick, and most users would not consider the software they access to be user friendly, except for the most simple and rudimentary tasks. Even the individuals who make a living utilizing the software (secretaries, writers, etc.) will usually acknowledge that they have mastered only a portion of the capacity of their programs.

Expanded IT in criminal justice agencies will face problems that are at least as large. The danger will be that officers will not have the time, inclination, training, and disposition to learn

what the IT demands, absorb what it offers, and incorporate it effectively into their daily work. In my opinion, this is the biggest single IT challenge for criminal justice agencies.

Knowledge and Risk

As noted above, the effects of IT advances in criminal justice agencies will have repercussions beyond the operational needs of the agencies themselves. One such side effect is a potential increase in knowledge about crime, criminals, and the criminal justice system. Most of us would consider this to be a benefit. But knowledge can be used for ill as well as good, and this risk looms particularly large at a time when misuse of personal data and assaults on personal privacy are already considered by many to be a major societal problem. We need to ask ourselves a number of questions. What is the balance between these two facets of the IT revolution in criminal justice agencies? Does the good outweigh the bad? Is there a way to maximize the former and minimize the latter? I will not presume to provide answers to these questions but I will try to outline their dimensions.

Better information gathering, processing and dissemination offers benefits in at least four distinct areas.

- *Strategic and Tactical Decision-Making By Criminal Justice Agencies.* This simply reiterates the theme that has been developed during this article. The more information an agency has and the better its methods of processing that information, the greater the likelihood that decision-making will be rationally based.
- *Cross-Jurisdictional Cooperation and Collaboration.* Good information will create a better foundation for effective cross-jurisdictional interaction. Agencies will be able to make a more effective contribution concerning their own knowledge and experience, and will also be able to better utilize information provided by other jurisdictions. Cooperation and collaboration on matters of common interest will be enhanced.
- *Aggregation at State, Regional, and National Levels.* Aggregate statistics such as those produced by the Uniform Crime Reporting system are no better than the quality of the data provided by individual agencies. Improved data at the local level leads to improved aggregations at higher levels. Better compilations and more accurate statements of trends will be the result.
- *Stimulation of Research.* A common complaint among researchers is that the research they do is not often used. There are a number of reasons for this. Some are ideological and not susceptible to easy change.[39] Others however are a consequence of the informational impediments that researchers have characteristically faced. These have tended to mean that research costs too much, takes too long, and produces results that are too often equivocal.[40] This is particularly true of research that has focused on police departments.[41] However, with more dependable and more comprehensive computerized data, policing research will be better positioned to increase our basic knowledge about crime, and inform policy-making at local, state, and national levels.

Few would resist the assertion that these improvements are desirable. Many would agree that they are necessary. Looked at from that point of view, these are side effects of the IT revolution that we can applaud. But we cannot leave it at that. We have to look at the other side of the coin. As information about crime, criminals, and suspects becomes more detailed and more easily accessible and manipulable, we must consider whether potential misuses of such information are possible, and if so what we should do about that.

I think there are three areas where the proliferation of information could lead to problems. These all involve matters of privacy and security of individuals.[42]

- *Inaccuracy of Data.* As more and more information is accumulated about individuals, it becomes increasingly important that the information be accurate and dependable. This isn't only true in the law enforcement world, of course. None of us want our good credit records to be reported as bad, for instance. But, when we are speaking of a law enforcement context, the negative effects of inaccurate or incomplete data about individuals can be devastating. Quite a lot of police departments collect data on possible gang members for instance. Some use a series of markers to assess likely gang membership (clothing, nicknames, tattoos, associates). Above a certain threshold (e.g. perhaps three out of four "hits"), the person is flagged as a gang member. There may be no known criminal activity associated with such a person, but the person may subsequently be treated as if there were. An argument can be made that the potential for the prevention and control of crime is enhanced by this procedure. But, it is not necessary to be anti-law enforcement or a gang sympathizer to be troubled by the approach. What if the information is inaccurate?
- *Unrestrained Official Use.* A lot of the information about persons that gets into police files is developed through investigation of complaints and crimes. Such development is a normal and proper exercise of police power and responsibilities. When this information is paper-based, access to it tends to be limited. Inside the department, neither civilian nor sworn staff spend their time rummaging through files about cases with which they personally have no association. And, departments would not, for instance, copy an investigative file and send it out to another agency or a business without a very good reason. But, when such information becomes computerized, it is an easy matter to apply different standards. It becomes a simple matter for data on individuals to be made available to other law enforcement agencies, to other public agencies that request it, to businesses, and perhaps even to individuals. All that is needed is for an officially approved reason to exist. The reason might be to check a would-be gun purchaser under the Brady Law; it might be to approve an application for a driver's license; or to make a decision about a job applicant; or to decide whether or not to rent an apartment. Some of these seem obviously legitimate uses of police data; some seem questionable. Either way, once transmitted, control of the information is lost. The information could go anywhere and be used for any purpose. Is this what we want?
- *Unauthorized Access.* A paper file in a filing cabinet or an officer's desk drawer has a symbolic boundary around it. Not only is it inaccessible to outsiders, it is not likely that unauthorized insiders will go looking through it. Such barriers disappear when the file is computerized. Insiders and outsiders have opportunities to get to it, sometimes without creating any record of access. If there is any doubt about this, it is only necessary to reflect on the number of known breaches of supposedly secure national databases by hackers. If hackers can get into files that are protected by national security systems, it's hard to see why computerized files in criminal justice

agencies will not be extraordinarily vulnerable. Obviously, this is not what any criminal justice agency (or any other law-abiding citizen) would want. But, it is hard to be confident that it could be stopped.

What this brief discussion suggests is that critical concerns exist about data quality and integrity, and about internal and outside access to sensitive information. Unrestrained or improper access seems certain to lead to abuses, and so deserves very careful attention. It may well be that dealing with these concerns may bring a limit to the amount and type of information that is considered proper to maintain in computerized criminal justice files, and/or in safeguards that may result in less than optimal technical use of the burgeoning IT capability. The risk at present seems to be that the rapidity of the movement towards computerization will outstrip the establishment of appropriate protections of individual privacy.

Conclusion

Among the many timeless observations made by Thomas Jefferson, one strikes me as having particular relevance to the criminal justice response to the IT revolution. On July 12, 1816, Jefferson wrote a letter to Samuel Kercheval, an extract from which is reproduced on one of the chamber walls of the Jefferson memorial. Jefferson said:

> I am not an advocate for frequent changes in laws and constitutions, but laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change, with the change of circumstances, institutions must advance also to keep pace with the times. We might as well require a man to wear still the coat which fitted him when a boy as civilized society to remain ever under the regimen of their barbarous ancestors.

Jefferson, of course, was making a very general point with this statement. But, taking a few liberties, I would propose that the situation he denotes is precisely the one facing criminal justice agencies. The human mind is advancing, it is producing new knowledge and capabilities at an astounding rate, and criminal justice agencies must keep up. The IT revolution and criminal justice agencies utilization of the capacity it generates is a journey not a destination. It may in fact be best conceived as a journey that has stops along the way. A certain amount of time will be spent at each stop, during which the features and amenities available at the stopping point are used, hopefully to good effect. However, sooner or later the features and amenities will become outmoded and inadequate. Then the journey will have to be resumed, and travel to the next stop will be required. At that next stop, what is available will be more advanced and, potentially, more helpful. It will also be more demanding.

This evolving process is going to be never-ending. There isn't going to be a point at which the ultimate destination has been reached. The amount of time spent at each stop is probably declining as the interval between each new advance diminishes. Criminal justice agencies are going to be continually challenged to adapt to changing circumstances, and, to a very significant extent, these circumstances are going to be circumscribed by information and the technology used to manage it.

In conclusion then, we must acknowledge that IS/IT and its uses by criminal justice agencies are continually expanding and seem virtually unlimited. The challenge for criminal justice agencies will be to take the (risky) step of dynamically embracing the new potential.

Endnotes

[1] During this paper I will use IT as a general shorthand term to designate information technology and its associated hardware and software elements.

[2] Asserting that the revolution has taken place in the past five decades is a practical construct that focuses attention on the development and contribution of the desktop computer, which was made possible by the invention of the transistor in 1947. It is not meant to do a disservice to earlier pioneers in the field, whose efforts were prerequisites for the desktop and the IT foundation that we take as commonplace today. This includes an array of seminal conceptual and practical developments, including, but not necessarily limited to, the following: Blaise Pascal's "Arithmetic Machine" (1642); Gottfried Leibniz's "Stepped Reckoner" (1694); Charles Babbage's "Analytical Engine" (1835); George Boole's binary logical operators (1859); Herman Hollerith's punched cards (1886); the Harvard Mark I created by Howard Aiken and IBM (1939); the ENIAC (Electronic Numeric Integrator and Calculator) created by J. Presper Eckert and John W. Mauchly (1946); the stored program concepts developed by John von Neumann in 1946 that in many respects opened the door to the logic underlying digital computer; and finally, of course, the development that ultimately made desktops and laptops a practical reality—the invention of the transistor in 1947 by Walter Brattain, John Bardeen, and William Shockley.

[3] For an excellent overview of IT developments and their relevance to the justice system, see J. David Coldren, "Change at the Speed of Light: Doing Justice in the Information Age," in "Computerization in the Management of the Criminal Justice System," Richard Scherpenzeel, Editor. *Proceedings of the Workshop and the Symposium on Computerization of Criminal Justice Information at the Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.* HEUNI, Publication Series No. 30, European Instititute for Crime Prevention and Control: Helsinki/The Hague, 1996. See also the many other articles in this document for a comprehensive examination of computerization and criminal justice issues.

[4] Decker, S.H., "Evolution of Crime Statistics as a Police Problem," *Journal of Police Science and Administration,* Vol 6, Issue 1 (March, 1978), pp 67–73. IACP, Alexandria, VA. This article provides a useful, though brief, overview of the historical development of statistical reporting on crime.

[5] A helpful summary of the UCR system can be found on the FBI Web page at *http://www.fbi.gov/ucr/ucrquest.htm.* The page provides responses to frequently asked questions about the UCRs, and is an excellent introduction to the topic. The bibliography to this article contains an extended list of references. An additional crime reporting system that has the potential for at least supplementing and perhaps replacing the UCRs was proposed and adopted in the mid-1980s. It came to be called the National-Incident-Based Reporting System (NIBRS) and is discussed below in Section 3.

[6] Publications on the Wickersham Commission are numerous. For an Internet reference, see the University Publications of America web site *http://www.upapub.com/guides/wickersham.htm.* This excerpts from Samuel Walker, *Popular Justice: A History of American Criminal Justice,* 2d ed., rev. (New York: Oxford University Press, 1997). For other selections, see: James D. Calder, *The Origins and Development of Federal Crime Control Policy: Herbert Hoover's Initiatives* (Westport: Praeger, 1993) and the National Commission on Law Observance and Enforcement (1931). Reports Washington, D.C.: U.S. Government Printing Office.

[7] The most significant of these was the Cleveland Survey of Criminal Justice. Led by Felix Frankfurter and Roscoe Pound, this inquiry produced *Criminal Justice in Cleveland* (Cleveland: The Cleveland Foundation, 1922).

[8] See the National Commission *Reports (op cit).* A fourteenth report, on a particular case of abusive police behavior, was suppressed at the time of the original publications, but was later released.

[9] For the original report of the Commission, see President's Commission on Law Enforcement and

Administration of Justice (1967). *The Challenge of Crime in a Free Society*. Washington, D.C.: U.S. Government Printing Office. For a recent perspective on the commission and its effects, see the report of the Symposium on the 30th Anniversary of the President's Commission on Law Enforcement and Administration of Justice—U.S. Department of Justice, Office of Justice Programs, The Challenge of Crime in a Free Society: Looking Back Looking Forward (1998). National Institute of Justice, NCJ 170029, Washington, D.C.: U.S. Government Printing Office.

[10] Reported by Joseph Foote, *An Overview for the Symposium on the 30th Anniversary of the President's Commission on Law Enforcement and Administration of Justice*, p. 3. Printed in The Challenge of Crime in a Free Society: Looking Back Looking Forward, op. cit.

[11] See *Summary,* page v, The Challenge of Crime in a Free Society, op. cit.

[12] A review of federal legislation from 1968 through 1994 can be found in Terence Dunworth, Scott Green, Peter Haynes, Peter Jacobson, and Aaron J. Saiger, *National Assessment of the Byrne Formula Grant Program, Report #2: The Anti-Drug Abuse Act of 1988—A Comparative Analysis of Legislation, National Institute of Justice,* December 1996, NCJ 163882, 63 pages. A more focused assessment of the legacy of the 1967 Commission is provided by Michael Tonry, in *Building Better Policies on Better Knowledge,* printed in Looking Back Looking Forward, op. cit.

[13] Tonry, op.cit., pp 113–114.

[14] LEAA was officially terminated on April 25, 1982 (see S. Rept. 98–220, p. 3). A vast literature on LEAA exists. For an entry to it, see: Richard S. Allinson, *LEAA's Impact on Criminal Justice: A Review of the Literature,* Criminal Justice Abstracts, December 1979, pp 608–648; Robert F. Diegelman, *Federal Financial Assistance for Crime Control: Lessons of the LEAA Experience,* Journal of Criminal Law and Criminology, 73:3, 1982, pp 994–1011; Malcolm Feely and Austin Sarat, *The Policy Dilemma: Federal Crime Policy and the Law Enforcemnent Assistance Administration* (Minneapolis: University of Minnesota Press, 1980).

[15] The Violent Crime Control and Law Enforcement Act of 1994, U.S.C. 18, Ch. 47, Sec. 320603.

[16] I refer here to the Arrestee Drug Abuse Monitoring Program (ADAM), the successor to the Drug Use Forecasting Program (DUF), which systematically collects and analyzes urine samples from arrestees in jails in 35 U.S. cities and then correlates the results with interviews of those arrestees.

[17] Brady, T. *The Evolution of Police Technology. Presentation to the Technology for Community Policing Conference,* hosted by the National Law Enforcement and Corrections Technology Center. Washington, D.C.: U.S. Department of Justice, June 1997.

[18] SEARCH. 1999. *Survey of Criminal History Information Systems, 1997.* NCJ 175041. Washington, DC: Bureau of Justice Statistics

[19] The Brady Act of 1993 (went into effect in 1994) was an amendment to the Gun Control Act of 1968. See U.S.C. Section 922.

[20] Bureau of Justice Statistics.1999. *Presale Handgun Checks, the Brady Interim Period, 1994–98.* NCJ 175034. Washington, DC: Bureau of Justice Statistics.

[21] Bezdikian, V. and C.L. Karchmer. *Technology Resources for Police: A National Assessment.* Washington, D.C.: Police Executive Research Forum, July 1996.

[22] Reuland, M.M. Information Management and Crime Analysis: Practitioners' Recipes for Success. Washington, D.C.: Police Executive Research Forum, 1997.

[23] See for instance, National Partnership for Reinventing Government, *Providing 21st Century Tools for Safe Communities: Report of the Task Force on Crime Mapping and Data-Driven Management,* Washington, D.C.: U.S. Department of Justice, July 12, 1999.

[24] See a number of articles by Rich, T.F.: "Crime Mapping by Community Organizations: Initial Successes in Hartford's Blue Hills Neighborhood." In *Crime Mapping Case Studies: Successes in the Field,* N. La Vigne and J. Wartell, eds. Washington, DC: Police Executive Research Forum, 1998; "The Chicago Police Department's ICAM Program." *Program Focus.* Washington, DC: National Institute of Justice, 1996. "The Use of Computerized Mapping in Crime Control and Prevention Programs." *Research in Action.* Washington, DC: National Institute of Justice, 1995.

[25] Mamalian, C.D. and N.G. La Vigne. "The Use of Computerized Mapping by Law Enforcement: Survey Results." *Research Preview.* FS000237. Washington, DC: National Institute of Justice, 1999.

[26] Reuland, op. cit.

[27] E. Poggio. et al. (1985). Blueprint for the future of the Uniform Crime Reporting Program: Final Report of the UCR Study. NCJ 98348. Washington, D.C.: Bureau of Justice Statistics.

[28] Roberts, D.J. (1997). "Implementing the National Incident-Based Reporting System: A Project Status Report." NCJ 165581. Washington, D.C.: Bureau of Justice Statistics.

[29] As of May 1997, in addition to the 10 states certified to report NIBRS data, 24 states were testing NIBRS and another 8 states were developing NIBRS programs for further exploration. In the next few years, Phase III of the NIBRS Project will seek to encourage NIBRS's adoption through several measures: devoting resources to instituting NIBRS reporting at several large local law enforcement agencies; providing technical assistance to agencies desiring to implement NIBRS; building "national dialogue" on NIBRS in an effort to increase awareness and understanding of the program; and produce a videotape demonstrating effective use of NIBRS data, using local agencies as exemplars.

[30] Manning, W.W. "Should You Be on the Net?" *FBI Law Enforcement Bulletin,* 66(1) (January 1997): 18–22.

[31] Goodman, M.D. "Working the Net: Exploiting Technology to Increase Community Involvement and Enhance Service Delivery." *Police Chief,* 64 (8) (August 1997): 45–53.

[32] Sulewski, K.E. "Faxback Response: Previous Question: How Has the Internet Helped Your Agency?" *FBI Law Enforcement Bulletin,* 66(1) (January 1997): 23–25.

[33] Ibid.

[34] Paynter, R.L. "Internet Connections." *Law Enforcement Technology,* 25(8) (August 1998): 28–32.

[35] Roberts, D.J. *Integrated Justice Information Systems for State and Local Jurisdictions: An Overview of Planning Activities for the Office of Justice Programs, US Dept. of Justice.* Washington, D.C.: Office of Justice Programs, July 1998.

[36] For example, see the following two examples.

North Carolina Department of Correction. "Officers Use Technology to Work More Closely With Police." http://www.doc.state.nc.us/NEWS/983news/JWAN.htm. This site documents North Carolina's Justice Wide Area Network (JWAN). JWAN, located in Hendersonville, NC, links the town's probation office, sheriff's department, police department, district attorney's office, day reporting center and other criminal justice agencies. Completed with a grant from the Governor's Crime Commission, this relatively simple network relies on laptop computers and custom adaptations of common software. Officers are able report electronically, share photos of probationers with other agencies, and search for offenders according to physical characteristics. Although officers now spend more time on reporting, they are more mobile and the information they provide is much more helpful to others in the office.

Stratton, N.R.M. "Birth of an Information Network." *FBI Law Enforcement Bulletin,* 62(2) (February 1993): 19–22. The All County Criminal Justice Information Network (ACCJIN) in Contra Costa, California, established in 1990, links 23 preexisting criminal justice information systems into a network. The network is composed of two message-switching computers, a private packet switching setup, and customized common software applications. The information system has radically improved all areas of criminal justice work in the county, from jail administration to dispatching to communication among offices (previously accomplished by fax and photocopy). The program's successful completion is traced to good communication, adequate funding, and effective definition of criteria.

[37] See, for instance, Declan McCullagh, *The Marker of a Criminal,* Wired Digital Inc., November 19, 1999. Accessible through: http://www.wired.com/news/politics.

[38] This process is already under way. The Office of Community Oriented Policing Services is planning a series of IT technical assistance conferences for the first six months of 2000. The objective will be to provide assistance to the departments receiving COPS funding under the COPS MORE program, which supports a variety of initiatives, IT development being one of them.

[39] See Jeremy Travis, *Criminal Justice Research and Public Policy in the United States,* in Scherpenzeel, op. cit. Pp 115–125.

[40] For comments on the general problems associated with research see Terence Dunworth, *National Assessment of the Byrne Formula Grant Program,* National Institute of Justice Research in Brief, p. 8. June 1977.

[41] For an illustration of the particular difficulties associated with policing research, see Terence Dunworth, *Crime in Public Housing: A Three City Analysis,* National Institute of Justice, 1993. This study began as a five city inquiry using police department data. Two of the five cities had to be dropped because the data did not support the spatial analysis that the project performed. In the others, Thomas maps were used to manually correlate police department data with housing development boundaries. In a more recent project, the advances made in police department data are illustrated by the fact that longitude/latitude coordinates were developed for more than 90% of specific incidents contained in city-wide databases in five cities for which such databases were obtained. See, Terence Dunworth et al, *The National Evaluation of the Youth Firearms Violence Initiative,* National Institute of Justice, 1999.

[42] A cross-national discussion of privacy and security issues can be found in Peter Csonka, *Council of Europe and Data Protection: Free Flow of Information versus Privacy,* in Scherpenzeel, op. cit, pp. 103–112.

LOOKING AT THE LAW

By David N. Adair, Jr.
Associate General Counsel, Administrative Office of the U.S. Courts

Cyber Searches

Any discussion of technology, particularly the use of computers in criminal activity, raises questions about how that use affects traditional means of monitoring compliance with conditions of pretrial release, probation, and supervised release. Officers supervising persons charged with or convicted of offenses that involve computer use are naturally concerned about protecting the public from further criminal activity. There is particular interest in monitoring compliance by means of searches of defendants' and offenders' computers and in installing on those computers software that captures certain information about how the computers have been used. But these are areas that have been given virtually no attention in either reported cases or professional literature. Consequently, it is not possible to provide any definitive discussion of the law regulating these kinds of supervision techniques. This column, instead, will offer a few observations and suggestions pending developments in the area.

First, while nothing is yet entirely settled in this area, the fact that information is stored in computerized form does not make it less subject to the Fourth Amendment protection against unreasonable searches and seizures.[1] Individuals have a reasonable expectation of privacy in such information, just as they have an expectation of privacy in physical materials and documents in their homes and offices. In fact, searches involving computers exacerbate the invasion of the privacy of innocent documents inherent in most document searches.

Computers store vast amounts of information and computer records are extremely susceptible to concealment, tampering, or destruction. Accordingly, it is often more difficult in computer searches to access particular documents without observing others. As with physical document searches, this problem is accepted as inevitable, and inadvertent disclosure of innocent documents will not invalidate a search, but the numbers of records potentially involved makes it particularly important to be cautious and, prior to such search, to identify those records that are the object of the search.[2] The seizure and removal of computer hardware in order to conduct searches at another location, where expert assistance and equipment is available, can be extremely disruptive and requires adequate safeguards to reduce such disruption.[3]

That is why there has been so much judicial scrutiny of warrants for computer searches and of the execution of such warrants.[4] This scrutiny suggests that searches of computers must be narrowly focused so as to avoid unnecessary intrusions into the zone of privacy to which an individual is entitled. Of course, any searches conducted by probation officers would not be pursuant to a warrant, but would be accomplished by means of a valid consent or pursuant to a search condition. It is uncertain how principles governing warrants might apply to search conditions. Given offenders' reduced expectations of privacy, it is arguable that computer searches conducted pursuant to search conditions need not be as narrowly focused as searches conducted pursuant to search warrants. Nonetheless, until these issues have received judicial attention, a conservative approach to such searches is advised.

The authority of the probation officer to search without a warrant under certain circumstances was confirmed in *Griffin v. Wisconsin*.[5] In *Griffin*, the Supreme Court held that the warrant and probable cause requirements of the Fourth Amendment may be set aside when the special needs of the administrative agency are beyond the normal needs of law enforcement, the privacy interests of the regulated party are diminished, and the agency's special needs make a warrant and probable cause requirement impractical. The dual goals of probation—rehabilitation and security—justify close supervision to assure that the various conditions of probation are met. Since the probationer has been convicted and his liberty is dependent on the observance of the conditions, his expectations of privacy are diminished. The state's "special needs" outweigh the offender's interest in being free from searches conducted without a warrant based upon probable cause. Sufficient safeguards, such as those contained in the state regulation at issue in *Griffin,* should adequately protect the rights of the offender. The regulation at issue included a requirement that the probation officer have reasonable suspicion to believe that the search would produce contraband or evidence of a violation, and that the search be approved by a supervisor. There is no such regulation governing searches by United States probation officers, but a number of United States courts of appeals have determined that a search condition provides the requisite authority to satisfy the Fourth Amendment's reasonableness requirement.[6]

Model Search and Seizure Guidelines

In response to and consistent with this line of authority, the Judicial Conference Com-

mittee on Criminal Law approved the Model Search and Seizure Guidelines for probation officers. The model was authorized for distribution by the Judicial Conference in 1993. (March 1993 *Report of the Proceedings of the Judicial Conference of the United States*, p. 13.) Officers are not bound by the model unless adopted by the court in the officers' district, but the model does represent the judgment of the Criminal Law Committee, not only of the law in the area, but of an appropriate policy for the conduct of searches by probation officers. In general, the model discourages searches in favor of more traditional supervision techniques and provides a number of safeguards when searches are contemplated. These include the requirement of a search condition or a knowing consent, a limitation on searches to situations in which there is reasonable suspicion that contraband or evidence of a violation of conditions may be found, and approval by a supervisor.

There has been no revision of the model. While one may argue that the philosophy of very limited searches should give way to current circumstances, such as the increasing impact of the use of computers in crime, there is no indication that the legal basis for probation officer searches has changed. It still appears necessary that a probation officer search be authorized by an offender's knowing consent or a valid search condition.

The requirement of reasonable suspicion for a search has not been conclusively determined, but the uncertainty is no greater now than it was when the model was promulgated. The Criminal Law Committee relied upon the rationale of those cases that appeared to require reasonable suspicion as a prerequisite to a warrantless probation officer search unless the offender consents to the search.[7] The Committee also determined that such a standard was useful in limiting arbitrary searches and abuse of the search condition. In addition, it determined that a requirement of reasonable suspicion also would operate to clarify and focus the scope of the search.

Surveillance Software

This issue is confronted most directly in the context of surveillance software. This software either captures pictures of the material that an offender has been viewing or records the sites the offender has accessed. While I have found no authority regarding this software in the context of the Fourth Amendment protection against unreasonable searches and seizures, I think it reasonably clear that its use constitutes a search. The contents of a computer are protected from unreasonable searches and seizures under the Fourth Amendment. The software stores captured images or other information that would then be viewed by an officer on a periodic basis. If the inspection of the material stored in a computer is a search, it follows that the inspection of automatically preselected material is also a search.

The reasonable suspicion standard is implicated in this context because it is likely that the use of this type of software contemplates regular or random monitoring and that it will not be limited to situations in which officers have reasonable suspicion that an offender's computer contains contraband or evidence of a violation of conditions. Given the lack of certainty in the requirement of reasonable suspicion, and the fact that the use of such software is less intrusive than a full-blown computer search, it is understandable that some courts will want monitoring to be done without a necessity for reasonable suspicion. The model search policy requires reasonable suspicion for searches generally, but does allow for random, routine, or periodic searches only if specifically authorized by the court in the search condition. Accordingly, I suggest that such monitoring should be conducted pursuant to specific court authorization in the form of a special condition that permits the use of the particular software. And, if it is the intent of the court that the results will be monitored by a probation officer on a regular or random basis, the condition should specifically so state.[8]

The issue of searches by pretrial services officers deserves mention. It is not entirely clear that the *Griffin* analysis justifies warrantless searches of defendants by pretrial services officers, but this issue has been treated elsewhere.[9] Of course, should a court determine that the authority to conduct such searches exists and imposes a search condition of pretrial release, the same considerations regarding computer searches would apply to pretrial services officers as probation officers.

Special Search Conditions

No matter what the kind of supervision, the imposition of a search condition must be supported by information that it is necessary to have a special search condition imposed by the court based upon the individual needs of the offender. The provisions that permit discretionary conditions of pretrial release, probation, and supervised release all provide that conditions that involve deprivations of liberty should be no greater than are reasonably necessary to the rehabilitation of the offender and the protection of the public.[10] Two recent cases highlight the importance of a discrete and carefully focused use of special conditions that infringe on an offender's liberty.

In *United States v. Peterson*,[11] the defendant was convicted of passing bad checks, and also had a three-year-old state incest conviction. The conditions of his probation included a prohibition on access to the Internet (he also was in the habit of viewing adult pornography) except for employment purposes as approved by the probation officer; sex offender treatment; third-party notification of employers; and a prohibition on being in various places where children congregate. The court struck down the ban on Internet access. It relied on the provisions of 18 U.S.C.§ 3563(b), which permit conditions that involve deprivations of liberty as necessary for the rehabilitation of the offender and the protection of the public, as well as deterrence and punishment. The court held that the Internet ban was not reasonably related to the offense of conviction or even the earlier offense, and was not reasonably necessary to protect the public.

The court distinguished *United States v. Crandon*,[12] where the computer limitations were closely related to the offense of conviction. There, the defendant had used the Internet to lure a minor to his home, where he molested her. The court also struck down the sex offender treatment, but only because the language of the condition did not make clear whether the probation officer had the authority to decide on treatment or not, or was simply to approve the type and place of treatment. It also struck down the limitation on the offender's frequenting places where children might congregate as not reasonably related to the earlier offense.

In the second case, *United States v. White*,[13] the offender had been convicted of receiving child pornography. Among his conditions of supervised release, the offender was required to undergo sex offender treatment, refrain from the possession of erotica, refrain from possessing a computer with Internet access, and submit to searches. The court struck down the computer condition because, it reasoned, Internet access is so very important today, much like the telephone. The defendant confirmed its importance by arguing that he needed the Internet to research the book that he had suddenly decided to write. As in *Peterson*, the Tenth Circuit distinguished

Crandon since the use of the computer was much more a part of the offense in that case. The court suggested, instead, the use of filtering software. It recognized that filtering might be defeated by a clever offender, but appropriately recognized that no condition can be guaranteed to be perfectly effective. At the same time the court dismissed the challenge to the search condition with very little discussion.

These cases demonstrate that a condition that infringes on the rights of an offender must be carefully designed to meet the needs of the offender and not infringe upon those rights more than is necessary. In the cases cited, the conditions imposed by the district courts did not appear sufficiently related to the offender's individual circumstances. The sentencing courts may have seen the defendants simply as "sex offenders" and imposed a package of conditions without considering their individual circumstances. These cases do not prohibit the imposition of conditions limiting access to the Internet, but they will likely make such imposition more difficult. They suggest that improvidently imposed search conditions or improvidently conducted searches under such conditions might serve as the vehicle for successful challenges on officer searches. Accordingly, it is suggested that, particularly while the law develops in this area, officers be very cautious in recommending search conditions or other conditions that impinge on offenders' liberties only to those offenders who the officer believes present a particular danger to the public or who have a particular propensity to re-offend.

Statutory Limitations

In addition to constitutional limitations, there are also statutory limitations to computer searches. The Electronic Communications Privacy Act (ECPA) is the most significant of these for probation and pretrial services officers. The ECPA has two parts. Title I is an amendment to the wiretap provisions located at 18 U.S.C. § 2510 *et seq.* and deals with the interception of transmissions. The term "interception" has been very narrowly defined, and is unlikely to apply to anything that an officer is likely to do in the course of supervision.

Title II of the ECPA (18 U.S.C. sec. 2701 *et seq.*) deals with access to stored electronic communications. It requires a warrant and advance notice for most searches covered by the act. But title II applies only to the accessing of communications electronically stored in an electronic communication service. Such a service is one that provides computer storage or processing services to the public. The act is designed to protect the privacy interests of the innocent users of such services. The act would cover, for example, intra-company networks, electronic bulletin board systems, and other on-line systems. It would not ordinarily include personally owned, or stand-alone, computers even though they may be used to send and receive communications by means of an electronic communications service.

But care should be taken in accessing e-mail messages. Where e-mail has been received by a recipient's service provider, but has not yet been accessed by the recipient, it is in temporary electronic storage and is protected by the provisions of the ECPA.[14] If the recipient accesses an e-mail message, and it is retained on the recipient's hard drive, it is no longer covered by the act. But if opened e-mail is retained on the provider's system, it is considered to be in a remote computing service under the ECPA and is protected. It is not clear that a search condition is sufficient to authorize disclosure of e-mails that are in electronic storage or in remote computing systems, or whether 18 U.S.C. §2703 would authorize the court to order such disclosure in the context of pretrial release, probation, or supervised release. Officers may wish to consult with their courts if access to this kind of material is critical.

Conclusion

The potential for the discovery of incriminating information, particularly information that may relate to public safety, is clearly intriguing. At the present time, however, there is no justification for believing that an offender's computer is significantly more accessible to a probation officer than the offender's physical property. I use the term "significantly" advisedly, for nothing is certain in this area. There are arguments that an offender's reasonable expectation of privacy cannot be exactly the same for computerized information, since access to that information may be available when an offender uses the Internet. It is also possible that technology may provide a way to limit access to contraband information. Such a limitation could eliminate any reasonable expectation of privacy a person may have in the information. And it seems likely that the rules for searches of physical property do not apply in the same way that they do to computer searches. But until there is more clarity in the area, probation officers should consider taking a conservative approach and limiting recommendations for search conditions in sex offender and other computer-related cases and in limiting computer searches to the extent that they would do so in other cases.

Endnotes

[1] *See*, 1 LaFave, *Search and Seizure* § 2.6(f) (3d ed. Supp. 2001) and, for a good discussion of the subject generally, Winick, *Search and Seizures of Computers and Computer Data*, 8 Harv. J. L. & Tech. 75 (Fall 1994).

[2] *See, e.g., United States v. Gray*, 78 F.Supp.2d 524 (E.D.Va. 1999); *United States v. Hunter*, 13 F.Supp.2d 574 (D.Vt. 1998).

[3] *See, e.g., Steve Jackson Games, Inc. v. United States Secret Service*, 816 F.Supp. 432, 437 (W.D.Tex. 1993), *aff'd.* 36 F.3d 457 (5th Cir. 1994).

[4] *See,* Winick *supra* note 1, at 101.

[5] 483 U.S. 868 (1987).

[6] *United States v. Wryn*, 952 F.2d 1122 (9th Cir. 1991); *United States v. Giannetta*, 909 F.2d 571 (1st Cir. 1990); *United States v. Schoenrock*, 868 F.2d 289 (8th Cir. 1989); *United States v. Robinson*, 857 F.2d 1006 (5th Cir. 1988). For a full discussion of this issue, *see*, Adair, "Probation Officer Searches," 62 *Federal Probation* 68 (June 1998).

[7] *See, United States v. Giannetta*, *supra* (the court noted that a lack of a standard for searches in the search condition may have rendered the condition overbroad, but held that since the actual search was based on reasonable suspicion, the search was unobjectionable). *But see, Owens v. Kelly*, 681 F.2d 1362 (11th Cir. 1982) (in a decision rendered before *Griffin*, the court rejected a reasonable suspicion requirement for a state probation search).

[8] A search might be conducted without probable cause with the consent of an offender. The model search policy, however, contemplates that even a consent search should be conducted only upon reasonable cause.

[9] *See,* Adair, "Probation Officer Searches," *supra. See, also, State v. Ullring*, 741 A.2d 1065, 1072 (Maine 1999) (applying the *Griffin* analysis to hold that pretrial warrantless searches are constitutional).

[10] 18 U.S.C. §§ 3142(c)(1)(B), 3563(b) and 3583(d). It has always been the law that conditions of supervision should meet the needs of the individual offender. *See, e.g., Owens v. Kelly*, 681 F.2d 1362, 1366-67 (11th Cir. 1982): *United States v. Consuelo-Gonzales,* 521 F.2d 259, 263 (9th Cir. 1975) (*en banc*). And this remains the law under the Sentencing Reform Act. *See*, S. Rep. 98-225, 98th Cong., 1st Sess. 94-95 (1983), *reprinted in* 1984 U.S. Code Cong. and Admin. News 3277-78.

[11] 248 F.3d 79 (2nd Cir. 2001).

[12] 173 F.3d 122 (3rd Cir. 1999).

[13] 244 F.3d 1199 (10th Cir. 2001).

[14] *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d at 461-462.

IT HAS COME TO OUR ATTENTION

TechBeat

NIJ's National Law Enforcement and Corrections Technology Center now publishes a quarterly newsletter, *TechBeat*, "dedicated to reporting developments in technology for law enforcement, corrections, and forensic sciences." *TechBeat* can be accessed online at www.nlectc.org, or can be received by mail at no cost by calling 800-248-2742 or by e-mailing them at asknlectc@nlectc.org. Among the topics discussed in the Spring 2001 issue were:

- **NYC Probation on Track**—The New York City Department of Probation recently introduced a new classification system for its offenders that includes a low-risk Reporting Track largely serviced through automated reporting kiosks. After the offender's initial face-to-face meeting with the probation officer, contacts are made using one of 14 kiosks among five probation offices. In less than three minutes, offenders can check in at the ATM-like machine, and update their records. The computer program has a database that allows it to check the offender's information for errors, freeing officers for more time-consuming work with higher-risk cases. And failure-to-report rates have dropped form 50 percent per month to 10 to 15 percent.

TechBeat also includes "Tech Shorts," a summary of relevant technology items that have appeared in publications around the country. The Spring 2001 issue included these stories:

- **Use of DNA Evidence Expands** (from the *Milwaukee Journal Sentinel*)—"DNA testing is being used more often in routine investigation . . . of burglaries, robberies, and kidnappings, since DNA can be taken from ski masks, saliva, cigarettes, and other items. . . . Police recently used blood on a broken window to trace a burglary to the case's suspect."
- **UV Light to Lock TB Out of Jail** (*Memphis Commercial Appeal*)—"Tennessee health officials announced that inmates at the Shelby County jail will be protected from airborne bacteria, such as tuberculosis (TB), by using new ultraviolet light technology to recycle the indoor air flow through several ultraviolet lights that will kill TB-causing bacteria. The system, which is used in water-purification and food-processing systems to reduce the risk of contamination, is being installed in the jail's heating and ventilation system."

Justice Technology Monitor

Another entry in the growing number of useful online sources of information for criminal justice professionals is *Justice Technology Monitor: The newsletter on technology & funding for law enforcement, court and corrections professionals.* This is a newsletter with a hefty subscription price (available from Capitol City Publishers, 1408 N. Fillmore Street, Suite 3, Arlington, VA 22201-3819, or ph 1(888) 854-3080), but you can access an online version at www.capitolcitypublishers. com. Among recent articles:

- **Grants Help States Reduce DNA Backlog**—"The National Institute of Justice (NIJ) Convicted Offender DNA Backlog Reduction program in FY 2001 will provide $8 million to rapidly advance the analysis of convicted offender samples collected by the states . . . consistent with federal and state databases. . . . Data will be reported in a CODIS-compatible format so that DNA profiles can be entered into state and national DNA databases."
- **San Diego Lab Pools Resources to Address Law Enforcement Priorities**—"The nation's first state-of-the art regional computer forensics laboratory officially opened recently, paving the way for new interagency cooperation to address the collection and analysis of computer evidence from crime scenes."

Recent Reports From NIJ

Several recent reports from the National Institute of Justice (NIJ) are likely to interest those in the fields of criminal justice and corrections. Among them:

- *The New Structure of Policing: Description, Conceptualization, and Research Agenda* (July 2001). This report describes worldwide restructuring of policing, and the effects of these changes on issues of justice, equality of protection, and quality of service.
- *A Resource Guide to Law Enforcement, Corrections, and Forensic Technologies: Office of Justice Programs and Office of Community Oriented Policing Services* (May 2001). This guide is designed for local administrators to help them make informed decisions about current and emerging technologies affecting the fields of law enforcement, corrections, and forensic science technology.
- *What Future for "Public Safety" and "Restorative Justice" in Community Corrections?* (June 2001). This report explores some of the challenges facing community corrections. For example, "Pursuing public safety requires community corrections to take a more proactive approach, to come from behind the desk into the community, yet thrusting corrections into the community may disrupt its social fabric." The report discusses balancing victim and offender needs, gaining the offender's acknowledgment of responsibility, and "reconciling 'what works' strategies that focus on the individual offender with a restorative justice and public safety emphasis on the offender as one strand in a web of community interdependency."

- *Understanding DNA Evidence: A Guide for Victim Service Providers* (May 2001). In light of the increasing role of DNA evidence in criminal cases, this brochure describes the value of DNA evidence for victim service providers, and discusses evidence collection, contamination, and preservation issues.
- *The Future of Forensic DNA Testing: Predictions of the Research and Development Working Group* (November 2000). This report describes past and present techniques in forensic DNA analysis, and discusses projected two-year, five-year, and ten-year milestones for DNA technology.

All of these reports (and many more, including earlier reports) can be accessed from NIJ's web page: www.ojp.usdoj.gov/nij.

Contributors
To This Issue

Arthur L. Bowker

United States Probation Officer, Northern District of Ohio. M.A., Kent State University. Author of "The Advent of the Computer Delinquent," *FBI Law Enforcement Bulletin* (December 2000).

Timothy P. Cadigan

Program Technology and Analysis Branch Chief, Federal Corrections and Supervision Division, Administrative Office of the U.S. Courts. Previously, PACTS Project Manager, Federal Corrections and Supervision Division, Administrative Office of the U.S. Courts. M.A., Criminal Justice, Rutgers University, Newark, NJ. Author of "Technology and Pretrial Services," *Federal Probation* (March 1993).

Terence Dunworth

Managing Vice President for Law and Public Policy, Abt Associates, Cambridge, MA. Coauthor of "National Evaluation of Weed & Seed—Cross Site Analysis" (NIJ, July 1999).

Darren Gowen

Integrity and Safety Section Chief, Program Services Branch, Federal Corrections and Supervision Division, the Administrative Office of the U.S. Courts. Previously, Probation/Pretrial Services Administrator (Home Confinement/Electronic Monitoring Services), the Administrative Office of the U.S. Courts. M.S., University of Southern Mississippi. Author of "Overview of the Federal Home Confinement Program (1988-1996)," *Federal Probation* (December 2000).

Cary Horrocks

Systems Manager, United States Probation and Pretrial Office, District of Utah. M.B.A., Brigham Young University.

Brian J. Kelly

Senior United States Probation Officer and Cybercrime Specialist, Eastern District of New York. B.S., St. John's University, New York.

Lanny L. Newville

Senior United States Pretrial Services Officer, Field Automation Specialist, Western District of Texas. Previously, Senior Probation Officer, Brazos County Community Supervision and Corrections Department, Bryan, Texas. B.A., Sam Houston State University, Huntsville, TX.

Thomas G. Ogden

Deputy Chief United States Probation Officer, District of Utah. M.A., Organizational Management, University of Phoenix.

Kirby Phillips

President, Alcohol Monitoring Systems, L.L.C. Previously, President, Life Loc, Inc. Graduate Gemologist, Gemological Institute of America.

Timothy M. Scharr

Senior U.S. Probation Officer, Special Offender Supervision Team, St. Louis, MO. B.S., Southwest Missouri State University.

Michael Eric Siegel

Senior Education Specialist, Federal Judicial Center. Previously, Assistant Dean of Faculty Development, University of Maryland, College Park. Ph.D., Tufts University. Author of "Probation and Pretrial Chiefs Can Learn From Leadership Styles of American Presidents," *Federal Probation* (June 2000).

Elaine Terenzi

Chief United States Probation Officer, Middle District of Florida. Previously, Deputy Chief U.S. Probation Officer, Eastern District of New York. M.B.A., New York Institute of Technology; M.A., New School for Social Research, New York.

Gregory B. Thompson

United States Probation Officer, Southern District of Indiana. M.A. in Criminal Justice, Indiana University, Bloomington.

United States Government
INFORMATION

Order Processing Code

***5876**

Federal PROBATION

a journal of correctional philosophy and practice

FAX YOUR ORDER TO
202-512-2250

PHONE YOUR ORDER TO
202-512-1800

MAIL YOUR ORDER TO
Superintendent of Documents
P.O. Box 371954
Pittsburgh, PA 15250-7954

IMPORTANT!
Please include this completed order form with your remittance

thank you for your order!

CUT ALONG DOTTED LINE

Please send me _____ subscription(s) to ***Federal Probation*** at $14.00 each ($17.50 foreign) per year. The total cost of my order is $_____.

Price includes shipping and handling and is subject to change.

_____
(PLEASE TYPE OR PRINT) NAME OR TITLE

_____
COMPANY NAME ROOM, FLOOR, OR SUITE

_____
STREET ADDRESS

_____
CITY STATE ZIP CODE + 4

_____
DAYTIME PHONE INCLUDING AREA CODE

_____
PURCHASE ORDER NUMBER (OPTIONAL)

Method of Payment

☐ CHECK payable to: Superintendent of Documents

☐ GPO DEPOSIT ACCOUNT _____

☐ CREDIT CARD ☐ Visa ☐ Master Card ☐ Discover

_____
CARD NUMBER EXPIRATION DATE

_____
AUTHORIZING SIGNATURE

FEDERAL PROBATION

Administrative Office
of the United States Courts
Washington, DC 20544