PRIVACY IN THE INFORMATION AGE

CMRC
CRIME MAPPING RESEARCH CENTER

A Guide for Sharing Crime Maps and Spatial Data

U.S. Department of Justice
Office of Justice Programs
810 Seventh Street N.W.
Washington, DC 20531

John Ashcroft
Attorney General

Privacy in the Information Age:
A Guide for Sharing Crime Maps
and Spatial Data

Julie Wartell and J. Thomas McEwen
Institute for Law and Justice

July 2001

NCJ 188739

NIJ

National Institute of Justice

Debra Stoe
Program Monitor

Dr. Tom McEwen is currently the Director of Research and Managing Principal for the Institute for Law and Justice. With over 25 years of criminal justice experience, he has coauthored *Crime Mapping and Crime Prevention,* developed mapping applications for police agencies, and conducted an NIJ evaluation on drug market analysis using mapping applications.

Julie Wartell is a Senior Research and Technology Associate with the Institute for Law and Justice. She has a master's degree in public administration with an emphasis in criminal justice, has completed a fellowship at NIJ's Crime Mapping Research Center, and has given extensive training and presentations nationwide to officers and analysts.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Preface

During the past decade, the criminal justice community realized the valuable analytic benefits of geographic information systems (GIS). As a result, in 1997 the National Institute of Justice (NIJ) established the Crime Mapping Research Center (CMRC) to promote the use of GIS throughout the criminal justice system.

Geographic information systems are a new and powerful technology that can enhance the ability of researchers and practitioners to identify problem areas and target scarce resources more efficiently. GIS also enable greater data-sharing capabilities within and among agencies and organizations, resulting in greater access by many to vast amounts of data.

Recognizing potential privacy concerns that could arise from data-sharing initiatives, CMRC held a 2-day Crime Mapping and Data Confidentiality Roundtable. As a result of this meeting, NIJ recognized the need for and supported the publication of a crime mapping and data confidentiality guidebook.

This report is designed to provide guidance to law enforcement personnel, researchers, and others who are creating and sharing crime maps. It contains real-life examples and illustrations contributed by various police departments that demonstrate a variety of techniques that promote privacy, crime mapping, and data confidentiality.

Acknowledgments

T his guide could not have been prepared without the ideas and efforts of a diverse group of people and agencies with interests and responsibilities for making crime information publicly available. The Crime Mapping Research Center at the National Institute of Justice (NIJ) has been a strong advocate for its development. The authors would especially like to thank Dr. Nancy La Vigne for her recognition that sharing crime maps and spatial data is an extremely important issue for the field. Dr. La Vigne initiated discussion on the subject through the Crime Mapping and Data Confidentiality Roundtable convened in July 1999 in which participants debated papers and provided insights into a variety of issues on sharing crime maps and spatial data. The authors of this guide benefited from the proceedings of the roundtable, some of which are quoted or referenced in the guide.

A good guide should include real-life examples. Several appear throughout the guide to illustrate points, and the authors would like to thank the contributors for their efforts, especially Tom Rich, Jenni Gardner, Deena Bowman-Jamieson, Chris Bruce, Liz Groff, and Julia Conley. Examples of crime mapping Web sites and disclaimers were provided by the following agencies: *Evansville* (Indiana) *Courier & Press,* Mesa (Arizona) Police Department, Oakland (California) Police Department, San Diego County Automated Regional Justice Information System, Salt Lake County (Utah) Sheriff's Office, Redding (California) Police Department, and Sacramento (California) Police Department. We are also grateful to many other analysts, police officers, and researchers who provided their varying experiences, ideas, and healthy debates to this important topic.

Finally, we would like to thank several reviewers—both inside NIJ and others—who provided useful critiques of this publication.

Julie Wartell

Tom McEwen

Contents

I. The Problem of Crime Mapping and Data Confidentiality

T he purpose of this report is to provide guidance on the issues of sharing spatial crime data and crime maps. The target audiences for this publication are law enforcement managers responsible for making decisions about what will be mapped, personnel responsible for mapping, researchers, and Web site developers. The discussion is intended to help these individuals make well-informed decisions for their agencies and jurisdictions. Topics addressed include the following:

■ The costs and benefits of providing maps to citizens, other agencies, and researchers.

■ Privacy issues and how to address them.

■ Development of local guidelines for Internet mapping and sharing maps and data.

■ Examples of agencies that have successfully done Internet mapping while safeguarding privacy and minimizing liability.

■ The need for disclaimers when providing maps and data on the Internet.

■ The importance of geocoding "hit rates"[1] and the need to disclose them when providing maps.

■ Other issues surrounding the availability of maps on the Internet.

Without a doubt, the public has greater access to information than ever before. People of all ages, races, and economic and educational levels can obtain a wide range of information from both the private and public sectors. One controversial type of information to which people now have access is crime-related data and maps. A 1997 Bureau of Justice Statistics study found that 35 percent of local police departments provided citizens with routine access to crime statistics or crime maps. For departments serving a population of 100,000 or more, this percentage went up to 80 percent.[2] The increase in data availability is the result of several technological and policing trends such as the following:

■ Numerous advances have occurred in geographic information system (GIS) applications. Advances include the Internet and Internet servers, easy-to-use software, and GIS on desktop computers.

■ Computer hardware is smaller and cheaper, but more powerful. The computers in private homes and small businesses today were inconceivable even 20 years ago.

■ Connections between users and the Internet have become simpler, faster, and cheaper. While 28.8 Kbps dial-up modems were considered fast a decade ago, the options for everyday users today include cable connections, digital subscriber lines (DSL), Integrated Services Digital Network (ISDN) lines, and T1 lines, the latter of which can reach speeds of 1.544 Mbps. The result is that larger files (such as map graphics) can be downloaded and viewed with greater speed and ease.

■ Internet use is increasing. Researchers' estimates of adult Internet users in the United States range from 75 million to 100 million per month.[3] People of all ages, professions, and backgrounds regularly get online at work, home, and school, as well as at libraries, Internet cafes, and airports.

■ Services such as America Online provide millions of novices—and experienced users—with easy connectivity and a friendly interface.

■ Diverse datasets can be merged more easily than in the past. Advances in desktop and professional geographic information systems have allowed law enforcement agencies and others to collect, manage, and analyze a wide variety of data. Accuracy and currency of geofiles have improved. Departments within a city or county (such as the tax assessor, utilities, zoning, and police) have become more willing to share data.

■ Software for desktop and Internet mapping has made great strides. The two most common GIS programs used by law enforcement are ESRI's ArcView and MapInfo's MapInfo.[4] Both products allow officers, analysts, and management to make and view maps and data in a graphical user interface (GUI) environment. In addition, Internet mapping may be as simple as posting map graphics (in .jpg or .gif formats) or as complex as interactive mapping done through special software or programming.

■ Statistical tools for analyzing spatial data are improving steadily. In the early 1990s, there was only one commonly used tool to determine crime hot spots. Today, several are available, and they offer increased functionality and ease of use. More practitioners and researchers are taking advantage of these and other statistical tools in their everyday work.

The community has a desire for access to timely data about crime and other problems. In the past, elements of the community, such as victims, employers, and community-based organizations, were able to obtain certain types of crime data. Criminal histories, crime and accident reports, and statistical summaries and tables were provided, sometimes for a fee. Today, partly encouraged by community policing, other groups of people—residents, businesses, and visitors—are looking for more extensive crime-related information. One survey found that "most [people] are willing to give up some privacy protection if the tradeoff results in a benefit to the public, such as increased safety, crime prevention, or the protection of children."[5] Many citizens are taking an active interest in the welfare and safety of their communities. Police and citizens are working together in many communities to solve local problems. Crime-related information has always been a popular subject for the public. It may be a factor in deciding where to live, go to school,[6] or walk alone at night. Mapping is one tool that helps people learn about crime in their community.

Crime mapping and GIS have also become popular applications within the law enforcement community. In the past decade, law enforcement agencies have shown an increasing interest in a variety of information technologies. Besides the general excitement about using new technological "toys," there is good reason for this growing attention. Police operations are information driven. Police officers and administrators are more comfortable with technology and its use for analysis and decisionmaking than ever before. Police would like to use technology such as the Internet to reduce requests on staffing yet still provide services to the community. Expanded functionality in computer-aided dispatch and record management systems, mobile data terminals, the Internet, and GIS have allowed law enforcement to more easily share data and partner with people and organizations in problem solving.

However, these technological developments and the increased desire to share data and maps have caused several of the following problems to emerge:[7]

1. Citizens have a right to know about crime in their communities, but victims

have a right to privacy about what happened to them. How can those rights be balanced?

When a law enforcement agency posts a map of crime incidents on the Internet, it runs the risk of including too much or not enough data. For example, if a sexual assault victim's incident location is provided, then his or her identity can be determined, and his or her privacy has been violated. Yet if a sexual assault is not posted and subsequently an individual falls victim to a sexual assault, has the agency thwarted the public's legitimate interest? That is, in not publishing the risk of sexual assault in an area, is the agency failing to let would-be victims know they are at risk so they can take appropriate precautions?

2. Other interested persons, especially researchers, want access to geocoded data on crime. How can the data be provided without violating victims' privacy?

Researchers are accustomed to signing agreements to ensure the confidentiality of individuals when analyzing survey data, but such agreements are not prevalent regarding geocoded data. The field has yet to agree on what restrictions should be placed on researchers' use of data that will safeguard confidentiality while enabling researchers to spatially analyze [data using] rigorous methods—methods that ultimately serve the entire criminal justice field.

3. If geocoded data are made available to others, what are the potential negative social outcomes and accompanying liability issues associated with misuse of the data?

Disseminating crime maps to the public could revitalize informal redlining methods employed by some insurance and banking companies. Whereas a neighborhood identified as a high-crime area could be targeted for various types of positive local interventions, it could also be flagged as undesirable, resulting in residential flight and ultimately causing more damage to an already problematic area. Further, the creation of crime maps or sharing of geocoded data that are inaccurate may result in false perceptions regarding the nature of a crime or public safety problem. Agencies already have published incorrect addresses of released sex offenders under Megan's Law, resulting in serious legal implications.

4. If police departments make crime data available on the Internet, what security measures need to be taken to minimize the risk of intrusion?

It is possible to set up password protection, firewalls, and search-and-query options that block the display of particularly sensitive fields. However, police departments and officers are skeptical about the prospects of ensuring that intelligence information and other restricted data do not end up in the wrong hands.

These are the tough issues that police administrators, with input from researchers, the community, and other stakeholders, must answer. Because laws vary by State and municipality and policies vary across agencies, personalities, and situations, there is no one right answer.

The contents of this guidebook are based on a range of resources, including papers prepared by researchers and practitioners across the Nation and discussion notes from the National Institute of Justice's (NIJ's) Crime Mapping Research Center (CMRC) Crime Mapping and Data Confidentiality Roundtable held in July 1999, reviews of how other Federal agencies have approached similar problems, an assessment of crime mapping Web sites of law enforcement agencies, various articles, and panel discussions held at three mapping conferences sponsored by CMRC.

II. Making the Data and Maps Available

Law enforcement agencies throughout the United States have been providing crime maps and data to the public for many years. Every department has its own policy on what data can be released, in what form, and to whom. Policies are shaped by the Freedom of Information Act,[8] State law regarding public records, and each agency's philosophy. The use of the Internet to provide maps and data to the public has heightened the debate over whether such sharing should occur and, if so, how.

Bryan Vila, a professor at the University of Wyoming, proposes that "in modern society, technology holds the key to privacy."[9] Technological growth and innovation have put law enforcement in a position that no one would have imagined only 20 years ago. While the opportunity for increased access to crime data has come about through database integration, geographic information systems, and the Internet, policing as a field is also changing to meet the demands of the information-driven public. Law enforcement has been forced to adapt to these trends while still safeguarding the privacy of crime victims.

Why should a law enforcement agency make data and maps available to researchers, other agencies, and the public? There are many advantages, including the following:

1. *Providing crime maps through the Internet or another convenient mechanism actually may reduce police workload; that is, fewer calls may be made to the crime analysis section for special requests if the maps are readily available.* The Tempe (Arizona) Police Department put a variety of crime maps and information on the Internet to "provide timely information with nearly instantaneous updates and conserve time and resources by reducing mailings and virtually eliminating printing and duplicating costs."[10] In addition, making crime maps and statistics accessible will alleviate common citizen calls such as "Is this neighborhood safe?" by allowing the agency to refer the citizens to the Internet to make their own judgments.

2. *Many police departments have found that the more the community knows about crime and safety issues, the more willing it is to work with the police to solve those problems.* In addition, potential victims of a crime pattern may protect themselves better if they are aware of the problem.

3. *Maps can assist in community policing and problem solving by showing where problems do and do not exist.* While researching gang territories, George Tita, formerly with Carnegie Mellon University, mapped various activity spaces and found that only small portions of a neighborhood were affected. When he shared his maps and results with community developers and gang streetworkers, their response was that if this information was shared with everyone, people would understand that the whole neighborhood was not gang infested, and businesses might be more likely to operate and invest in the area.[11]

4. *Maps can increase public awareness about neighborhood problems.* On one hand, residents of higher crime areas may not want their problems highlighted. On the other hand, some welcome the attention: "I know that I live in a high-crime area, and [your] publishing the

information has only confirmed my opinions. However, it is satisfying that the local council is working in partnership with the police to accurately identify crime hot spots and as a result target crime prevention resources to those areas that most need it, rather than to the middle-class areas where people are more likely to sit on some local committee, shout the loudest, and get funds allocated to an area that in reality is of low priority."[12]

5. *Maps facilitate partnerships with researchers and other agencies.* If researchers lack accurate, current data, they cannot assist departments and the policing field in analyzing and solving crime and disorder problems. Most people recognize the advantage of sharing data among law enforcement agencies and across jurisdictions (because criminals do not usually respect city boundaries).[13] In addition, agencies outside of law enforcement, such as public housing, schools, hospitals, parks and recreation departments, and urban planning divisions can work toward community safety if they are better informed about crime.

6. *By providing maps and data, a police department can be sure the data are presented accurately.* If the department does not provide maps and data, someone else (such as the media or a neighborhood group) eventually will—then the department risks having its data interpreted and displayed by someone less familiar with them. One nongovernmental Web site that currently displays crime maps and data is APBnews.com (*http://www.apbnews.com/resource center*). Its data contain information and ratings from the CAP Index, a privately developed crime-risk database.

7. *Providing maps and data to the public is a means to hold the police department accountable.* By making information public, law enforcement agencies are less likely to risk altering the statistics to make themselves look better. In addition, the more the public knows about crime, the more likely it is that someone

or some group will ask what the police or, in a true police-community partnership, they can do about it. The concern by officers that the public may have access to up-to-date crime information has led to more internal requests for maps and use of Internet sites by the officers themselves. Officers do not want to be confronted by a community member who is more aware of crime in the neighborhood than they are.

Providing crime maps and data also poses several potential and actual disadvantages such as the following:

1. *The information might be used for commercial purposes* (e.g., alarm companies calling burglary victims), which many citizens may find a violation of privacy or a nuisance. Many departments already release lists of crime incidents to the media, and companies will still not be able to identify specific households from the map, but they could target general areas.

2. *Potential offenders may use crime maps to identify areas that have not been targeted and therefore may not be receiving much police attention.*[14]

3. *Crime maps could conceivably harm a high-crime area by reducing property values or increasing insurance rates.* However, no definitive study of the property value concern has been made, and insurance companies (at least in California) have already been using ZIP Code crime information for years to define rates. Taxi drivers, pizza deliverers, and other service people sometimes hesitate to go to high-crime areas, but their reticence is often based more on reputation than on hard data. Crime maps could alleviate concerns.

4. *Crime maps are open to misinterpretation by viewers if the maps are too complex or viewers do not understand statistics or crime data.* Further, map shading sometimes suggests that an entire area (e.g., beat, neighborhood) has a crime problem, when in fact all the crimes may be concentrated in one or two blocks.

American police agencies are not the only ones wrestling with the idea of providing crime data and maps to the public. Several countries in Europe have examined the issue and concluded that aggregate data, statistical tables, and hot spot maps should be released, but that privacy laws outweigh the public's right to know specific information.[15] In the United Kingdom (UK), the Data Protection Act of 1998 and the Crime and Disorder Act of 1998 spell out the principles for data exchange and release. In general, when data are shared across agencies in the UK, the victim's name and street number are deleted, leaving only the street name and city or town, in an effort to depersonalize the record and overcome any privacy issues.

With regard to maps of crime and crime-related data, specific privacy issues need to be examined. Although some of these issues have existed as long as crime incident and arrest data have been public records, others have arisen because of the distribution of maps and easier access to crime data. Privacy issues include:

- If a map shows the exact location of an offense, such as the victim's residence, or the incident address is released, the victim may be retraumatized by the fear that criminals will see him or her as an easier target.

- Victims may decline to assist in investigations and prosecutions if they believe offenders or their associates can find out where they live by looking at crime maps.

- If a person is victimized again, he or she may decide not to report the offense because of concerns about publicity through a crime map. An increase in unreported crimes makes it harder for police to respond to public safety concerns.

- Incident-specific details associated with a map could be misused. If specific addresses are identifiable, all privacy

is essentially eliminated. Agencies have found different ways to provide valuable information while still respecting privacy. Innovators include the Sacramento Police Department, Illinois State Police, San Diego Police Department, San Diego County Automated Regional Justice Information System (ARJIS), and Cambridge (Massachusetts) Police Department, along with an Oklahoma City television station.

Illinois State Police

Driven by a mandate to make registered sex offender information available to the public, in November 1999 the Illinois State Police (ISP) began providing Illinois registered sex offender information over the Internet. As of July 1, 2000, users had the ability to view photographs of registered sex offenders, as well as name, address, date of birth, and type of offense (either child or adult offender). The ISP believes that by placing this Internet tool in the hands of the field and general public, it will empower individuals, as well as strengthen partnerships through information sharing and open communication.

Also available on the site are crime and traffic information. By limiting the detail of fatal crash information available, ISP protects the rights and dignity of fatal crash victims and their families while still informing the public about highway safety issues. Currently, the user queries the system by choosing a level of geography to view, as well as date and certain crash criteria such as crash cause.

Returned is a variety of information regarding the basics of crashes, including time of day, day of week, whether a teen driver was involved, and whether alcohol played a role. Crime data consist of county aggregated Uniform Crime Reports incidents.

Users are able to see thematic views of the state, representing various index crimes by county. In this way, crime trends for the state are discernable but incident specifics remain private.

By Jenni Gardner, Strategic Information Analyst, Illinois State Police

The Sacramento Police Department *(http://www.sacpd.org)* had the first interactive crime mapping Web site. The site allows the user to choose by crime type, other geographic data layers, and area for a 3-month period. The Illinois State Police *(http://samnet.isp.state.il.us/ispso2/samintro.htm)* is one of the few State law enforcement agencies with crime maps available through the Internet, offering the public a variety of traffic, crime, and sex offender data. (See "Illinois State Police.") While the San Diego Police *(http://www.sannet.gov/police)* posted a wide array of static neighborhood crime maps and statistics in 1996, ARJIS *(http://www.arjis.org)* has recently taken this to the next level, becoming the first regional interactive crime mapping Web site—with information from all law enforcement agencies in the county. The unique quality of the Cambridge Police Department Web site *(http://www.ci.cambridge.ma.us/~CPD/)* is that, in addition to monthly crime maps, it was the first agency (and is still one of the few) to post updated crime pattern and trend maps to allow the public to assist in problem solving. (See "Cambridge Police Department.") The Oklahoma News 9 Web site *(http://www3.kwtv.com/television)*, one of a handful of nonlaw enforcement agency sites providing Internet crime mapping, uses data collected from a number of cities in the metropolitan area. The public can choose to view maps by crime and address.

Some lessons have been learned along the way. At first, Sacramento, Dakota County (Minnesota), and Durham (North Carolina) provided too much information on their Web sites. In those instances, the GIS information provided was not crime related; the

---

Cambridge Police Department

The primary beneficiaries of crime analysis knowledge have, in almost every agency, been identified as the patrol and investigative divisions. Knowledge is received from the community but not returned to it. However, regarding the community as a true partner in crime prevention and crime reduction requires giving it the same quality and quantity of information that the department would make available to its patrol officers and investigators.

The emphasis at the Cambridge Police Department (CPD) website is on content, not design. Although CPD would like to offer an interactive mapping feature and a searchable database, those features are currently beyond the ability of the department's crime analysts. What CPD does offer are reviews of almost every pattern, series, hot spot, and trend that we identify; stories of notable crimes and arrests; and reviews, updated weekly, of five of the city's most serious target crimes [specifically selected types of crimes].

Providing information in this fashion requires a certain amount of discretion. CPD is careful never to post anything that would compromise a victim's privacy. A victim's name is never included and an exact address rarely included, even when such information is available through other public sources. Since pin mapping is usually done on a citywide level, identifying an exact residence from a pin map is usually impossible. More delicate privacy concerns surrounding cases of sexual assault are almost never an issue since patterns of such crimes are comparatively rare in Cambridge.

CPD also never publishes information that would compromise an investigative or patrol strategy designed to apprehend an offender. For this reason, about 25 percent of crime patterns are not posted to the website until five to seven days after they are identified, and about 10 percent of patterns are never posted.

Beyond these considerations, CPD is inclined to give the public whatever information it has, even if it's potentially embarrassing to the department (as in the case of a pattern that's gone unsolved for months). Finally, CPD never offers statistics or maps by themselves—they are always accompanied by qualitative analysis.

By Christopher W. Bruce, Crime Analyst, Cambridge (MA) Police Department

Web sites provided public access to tax assessor/administrator information—in other words, the ability to search for property owners by name. Law enforcement and public officials were the ones who were apprehensive about their own privacy. In response to complaints, the City of Sacramento and Dakota County took the name search capability off the Web site but retain it in paper and mainframe records.

In several places, the data access debate has been taken to the courts. In North Carolina, although there is great concern about how the information is being used, State law "prohibits people interested in viewing public records from being required to 'disclose the purpose or motive for the request.'" Nevertheless, the Durham police chief led a successful effort to withhold his site's name search capability.[16] In 1997, California took the opposite approach when it enacted a law that prevents State and local governments from publishing the home address or phone number of any elected or appointed official on the Internet.

On the other hand, Milwaukee, Wisconsin, has a comprehensive GIS Web site *(http://www.gis.ci.mil.wi.us)* that includes information ranging from tax parcel ownership to crime to property violations to garbage routes. Cities and counties are finding that as more and more data are linked together and become readily searchable, the public gains easier access to information. Previously, most people found it too confusing or difficult to obtain such data, and therefore, these privacy issues did not arise. Currently, private and public organizations are more open to providing a wealth of information.

The State courts, another part of the criminal justice system, have also been grappling with the tension between providing criminal-related information and respecting privacy. In October 1999, members of Washington's Judicial Information System Committee held a hearing to review the State's judicial dissemination policy. One of the first attempts to address privacy concerns related to the electronic dissemination of judicial records; this discussion related to

a U.S. Supreme Court decision from 1989 involving the difference between paper and electronic court records and the extent of the release of personal identification information. In the *U.S. Department of Justice* v. *Reporters Committee* (489 U.S. 749) decision, the Supreme Court "embraced the notion that individuals had a privacy interest in the 'practical obscurity' of records concerning them. As applied to dissemination of court records, this meant that records available at the individual courthouses requiring hours of research to dig up would remain available to the public, but those same records should not be readily available on an electronic system that makes them accessible to anyone with a few keystrokes."[17] The courts, much like the police, are currently weighing public record, privacy, and dissemination issues based on who will use the information and how it will be used.

Issues and Guidelines

Although standards are beneficial in certain situations, in the case of local departments making crime maps and data available to the public, *guidelines* are more beneficial. Standards generally are requirements set by a local, State, or Federal entity by which organizations must abide. Guidelines are recommendations or pointers for informing and providing assistance. This document presents information to promote and encourage the proper use and distribution of maps and data and will assist an agency in addressing the above-mentioned questions and issues. Listed below are key questions that a police department may want to address before providing maps to the public, other agencies, or researchers.

■ Should data be provided on an address point basis or aggregated to a larger geographic area, such as a neighborhood?

■ What types of data should be mapped (e.g., crimes, calls for service, arrests, citizen complaints)?

■ Should data on juvenile arrests and victims be mapped?

- What other data should be shown on the maps, such as schools, parks, hospitals, public housing, bars, banks, or convenience stores?

- How often should maps be updated, and who within the department has the responsibility for updating them?

- What problems will viewers have in understanding the published maps and data, and how can interpretation be made easier?

- Because geocoding hit rates are seldom 100 percent, how can information about geocoding be conveyed to viewers?

- What cartographic decisions (e.g., symbols, scale, legend) need to be made?

For agencies that are new to GIS or to publishing information on the Internet and for those that want to know what to do, how to do it, and what to expect, the following are some suggested guides:

Decide which data to present

Point vs. aggregate data. Aggregating data solves the problem of identifying specific addresses and incidents. However, aggregating has two disadvantages. First, identifying a crime problem within the aggregated area is more difficult than when viewing point data. If an entire beat is shaded according to total incidents, one is not able to discern that only a few blocks within the beat may contain all of the incidents. This problem could be reduced by aggregating to the street segment or block level. Secondly, it is harder to conduct analysis and understand the relationship between two sets of data when they are aggregated at different levels, such as one at the beat level and the other at the census tract level. Two strategies that departments have used are plotting points representing crime incidents at midblock locations or including the 100-block address in the identifying table. If there is a concern for victim identification, one may need to be more careful about plotting point data in less densely populated and rural areas where there might be only one house on
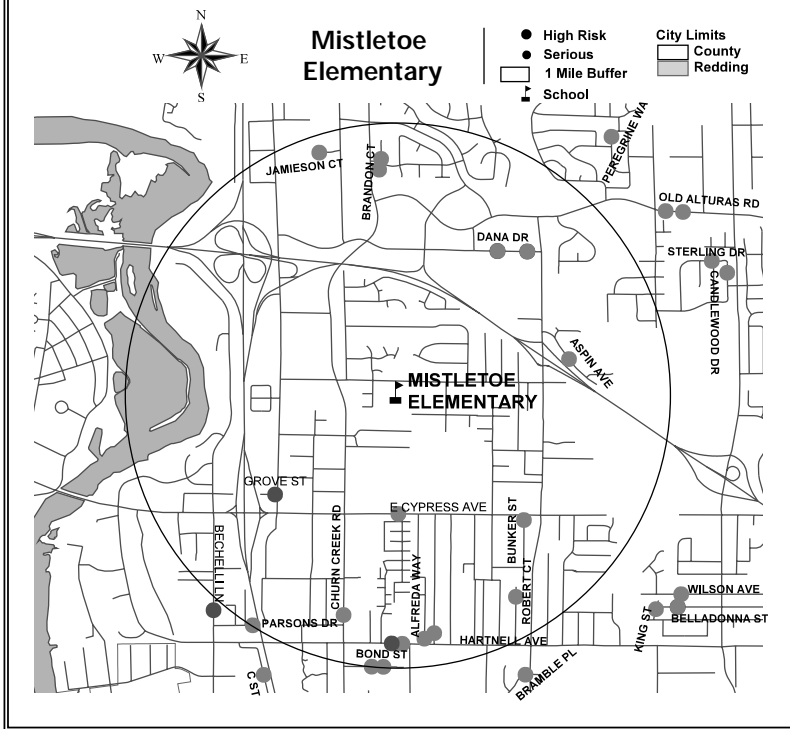
a street or one farm on several acres. Consideration should be given to the type of data that is being mapped; for example, not displaying child abuse and sexual assault incidents in this format.

Type of data to map and not to map. Most of the public would generally like as much information as possible, but that interest needs to be weighed against public record laws, privacy issues, and resources. Crime incident data are likely the most useful, but calls for service that do not usually turn into crime reports (such as noise complaints or shots fired) can also be useful. Although arrest data can be informative, arrest locations are greatly affected by police tactics and personalities, and explanations should be included. Departments should also consider providing data on traffic incidents, citizen complaints, code violations, and gang-related incidents.

Although many agencies are now using sex offender data for internal mapping and for investigations, State laws govern the release of such data to the public. With the passage of the Federal Megan's Law (P.L. 104–145) in 1996,[18] cities and States throughout the Nation began to make their sex offender registries available to the public. In most jurisdictions, this is done through a computer at the local law enforcement agency. In others, the information is placed on the Internet. (See *http://www. dps.state.ak.us/nSorcr/asp* for an example.) Generally, the data provided are name, address, date of birth, other personal information (e.g., eye color, height, weight), and type of offense. Some sites also have photographs, and a few have related maps. For example, on the Redding, California, Web site, *http://ci.redding.ca.us/rpd/ rpdmegan.htm*, maps show points that represent sex offenders living within 1 mile of a school. (See exhibit 1.) To identify specific sex offender information, a person must visit the police department to view the CD-ROM.

If a law enforcement agency is mapping sexual offender data, there is an additional issue to consider. The police agency is usually receiving the data from another agency,

Exhibit 1. **Sample Redding, California, Sex Offender Map**

can vary the area, the scale of the map, and the number of data types, users should be able to map a wider variety of data. Current technology allows the application to show different data and labeling according to the scale.

Use disclaimers

Disclaimers have traditionally been used to help avoid liability from misuse or misinterpretation of data. Some law enforcement agencies use a short disclaimer on every product they release—whether to officers or to the public. When an agency puts crime data and maps on the Internet, the potential users of that information increase a thousandfold, and this commensurately increases the need for a disclaimer. A disclaimer does not eliminate the liability risks, but it reduces them.

Unfortunately, there is no standard disclaimer for use with Web site crime maps and data, although several agencies have made initial attempts. (See appendix A.) When creating a disclaimer, a police department should consider where on the Web site to put it, whether users will be allowed to view the data and maps without acknowledging having read the disclaimer, and what the disclaimer should say.

Where to put the disclaimer depends on the other information on the Web site. Is the disclaimer meant to address only crime maps and statistics or all data posted? Is the disclaimer situated so that users have an option to read it or must read it (or pretend to read it) before they can use the maps or data? The wording is the most important concern. The department should describe as specifically as possible what it does not want to be liable for: the

such as a State department of corrections. The data may not be as accurate and timely as necessary to release to the public as the agency's own crimes, arrests, and calls for service. This could cause more problems, such as harassment of the wrong individual, than mapping an inaccurate auto theft. The use of disclaimers and explanations are especially important when mapping this data.

Juvenile data are important to problem solving, yet they present additional privacy concerns. Agencies should examine State and local laws specific to juveniles before moving forward; again, aggregating the data reduces the chance of identifying personal information.

The amount of data to present depends on the type of map—either static or interactive. On a static map, the graphic should not be too cluttered, and because it has an unchanging scale, only a set amount of information can be portrayed. Each agency must determine cartographically what the most important data will be for each map. For interactive mapping in which the user

information itself, the use and interpretation of the maps, and so forth. The department should consider including an explanation of geocoding, the department's accuracy rate, and the significance of that rate. Some agencies have turned to their legal departments for advice, some use other agencies' disclaimers as a starting point, and others create their own.

In addition to disclaimers, some organizations use privacy or confidentiality statements. Recognizing that new technologies such as the Internet allow the public to gain access to a great deal of information, the Federal Government directed all Federal agencies to post privacy policies on their agency Web sites in late 1999.[19] The memorandum states, "Each policy must clearly and concisely inform visitors to the site what information the agency collects about individuals, why the agency collects it, and how the agency will use it." One example of a confidentiality statement is the following excerpted from the U.S. Census Bureau:[20]

Sec. 9. Information as confidential; exception

(a) Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, or local government census liaison may, except as provided in section 8 or 16 or chapter 10 of this title or section 210 of the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Act, 1998:

(1) use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or

(2) make any publication whereby the data furnished by any particular establishment or individual under this title can be identified; or

(3) permit anyone other than the sworn officers and employees of the Department or bureau or agency thereof to examine the individual reports. No department, bureau, agency, officer, or employee of the Government, except the Secretary

in carrying out the purposes of this title, shall require, for any reason, copies of census reports which have been retained by any such establishment or individual. Copies of census reports which have been so retained shall be immune from legal process, and shall not, without the consent of the individual or establishment concerned, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding.

The National Archive of Criminal Justice Data uses the following combined privacy statement and disclaimer:[21]

This system and related software and equipment are intended solely for the communication, transmission, processing, and storage of National Archive of Criminal Justice Data (NACJD) information and data collections. For site security purposes and to ensure that this Web site remains available to all users, the Inter-university Consortium for Political and Social Research [ICPSR], NACJD's parent organization, monitors network traffic to identify unauthorized attempts to upload or change information or to otherwise cause damage to the site. Anyone using this Web site expressly consents to such monitoring.

Unauthorized attempts to modify any information stored on this system, to defeat or circumvent security features, or to utilize this system for other than its intended purposes are prohibited and may result in referral for criminal prosecution. If monitoring reveals evidence of possible criminal activity, such evidence may be provided to law enforcement personnel.

The views and opinions of authors expressed herein do not necessarily reflect those of the NACJD's sponsoring organizations, including but not limited to the United States Bureau of Justice Statistics and the United States National Institute of Justice.

With respect to documents available from this server, neither the University of

Michigan, ICPSR, or any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the University of Michigan, ICPSR, nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed.

Although a confidentiality statement does not protect an agency from liability, it serves as a promise to the public that a reasonable attempt is being made to protect their privacy. The use of a disclaimer in addition to the privacy or confidentiality statement allows an agency to inform the public of potential issues while also reducing the opportunity to lay blame on the provision of the data or the agency itself.

Provide information on geocoding rates

Geocoding is the process that enables tabular data to be used in a GIS. Geocoding is defined as assigning a location on the earth's surface. In simplest terms, if an incident report, for example, contains an address and the GIS contains a street centerline file (a computerized street map) with street names and address ranges (that contain the associated address), the computer can assign coordinates and map that record as a point. Since geocoding is a process, it can apply to either a single address or an entire data file.[22] The geocoding rate is the percentage of accurately matched addresses.

Providing the geocoding rate and an explanation of what it means on the map or on a Web site that contains multiple maps is important because the viewer will be more aware of the accuracy of the map and less inclined to misinterpret it. If the geocoding rate is only 75 percent, the viewer should question the usefulness of the map, and the law enforcement agency should take a serious look at its data. Even when the geocoding rate is 90 percent, there are probably key streets, areas, or addresses that are not matching for a reason. This

should be spelled out to the viewer. For example, if the base map (the computerized street file) has not been updated to include 700–999 Main Street and therefore no incidents appear, the map user should be informed so he or she does not believe that there are no crime incidents on those blocks. Tom Casady, chief of police in Lincoln, Nebraska, provides a realistic example: "Last year, police officers in Lincoln, Nebraska responded to 140,000 dispatches. If the source data were 100% accurate, and dispatch records were geocoded accurately 99% of the time, 1,400 dots would be misplaced on [or missing from] the resulting map."[23]

In addition, a simple explanation of geocoding should be provided along with the rate (otherwise, the rate will be meaningless). The viewer should be informed about interpolation (a computerized estimation of the distance along the street segment), street centerlines and offsets (the distance to the right or left of the street centerline), how multiple incidents at a mall or huge apartment complex are handled, minimum match score used (affects the accuracy of locations), and any address peculiarities that would cause nonmatches. Even with aggregate data, geocoding explanations and rates are important—especially for people whose address lies on a beat or neighborhood boundary. For a more extensive review of geocoding and address matching, see the Police Foundation's publication, Geocoding in Law Enforcement, on the Office of Community Oriented Policing Services (COPS) Web site at *http://www. usdoj.gov/cops/pdf/cp_resources/ e10990023.pdf.*

Provide guidance on how to interpret maps

With shaded (also called choropleth) maps, viewers must be informed that the data are grouped for an area and therefore are spread out evenly, unlike reality. Unless graduated symbols are used, point maps may be misinterpreted if the viewer does not realize that multiple incidents at the same address are all represented by one point. Hot spot maps are open to misinterpretation because

they are usually created using statistics that the viewers may not understand.

In addition, data sources and definitions should be discussed. Data on the map may represent crimes reported to the police, arrest locations, parolee home addresses that were reported to the department of corrections on their release, call-for-service locations, or gang contacts. Site designers need to remember that most of the public will not know the difference between a call for service (citizen request or complaint) and a crime incident (crime committed and report taken) or between an arrest location and the home address of the arrestee. Furthermore, not everyone knows what Part 1 crimes[24] are or even the difference between robbery, burglary, and theft. Staff should put themselves in the position of people not in law enforcement to determine appropriate explanations of terminology and cartography.

Basic cartographic design principles should be followed regarding symbols, size relative to the amount of data, and map scale. The symbol should be simple and understandable to the viewer and should be different for each type of data on the map. If symbols vary only by color and not shape, a person printing the map in black and white

---

Evansville (Indiana) Courier & Press Interpretation Guidelines

By looking at these maps, produced in cooperation with the Evansville Police Department, you can see where major crimes were reported in Evansville. Please note that not every reported crime will appear on the map. . . . [F]or the most part, the crimes pinpointed here are felonies.

Also note the maps include only crimes reported in the Evansville city limits. The locations as plotted are approximate and sometimes reflect the address of where a crime was reported, not where it was committed.

Retrieved March 20, 2001, from the World Wide Web: http://www.courierpress.com/crime.

---

will not be able to distinguish between data types. Graduated symbols should be used if there is a high frequency of multiple incidents at one address.[25] This type of symbology should also be explained, if used.

Map scale is another important element of data visualization. With interactive mapping, scale is determined within the application by the size of the area chosen and the size of the map-viewing section of the screen. In addition, the user may change the scale if the site offers zoom functionality (this allows the user to zoom in or out of an area). As mentioned earlier, some interactive applications allow different data and labels to appear, depending on scale.[26] If static maps are shown, the scale must be determined ahead of time depending on the size of the area and the amount of data on the map. Symbol size should be appropriate to the scale of the map.

The legend is important to the viewer. Without a clear, accurate legend, the map is useless. The legend should contain the symbols and descriptions of all data on the map, such as crime or call types, beat boundaries, schools, and police facilities. Graduated symbols, shading, and hot spot maps require specific symbol definitions. "*Evansville* (Indiana) *Courier & Press* Interpretation Guidelines," "Mesa (Arizona) Police Department Interpretation Guidelines," and "Oakland (California) Police Department Interpretation Guidelines" present interpretation guidelines currently provided at several crime mapping Web sites.

Encourage correct uses of maps, and keep them current

Because a major goal of providing maps to the public is education, the data must be current. The appropriate update frequency will vary by map type and amount of data. Static maps and databases used for interactive mapping applications should be updated at least once a month. Interactive mapping applications typically have an automatic mechanism for more frequent or even real-time updates. Static maps must be recreated and placed on the Web site, a process that often requires significant staff

resources; however, programs can be written to generate and post the same weekly or monthly maps in a semiautomated process (requiring a person to run the program). Jurisdictions with less crime may not need to update the maps as often, depending on the time period over which the data are portrayed. For example, *1 week* of crime incident data in New York City is about the same amount as *3 years* in Bismarck, North Dakota.[27] The responsibility for updating should fall on one person (such as a computer specialist, analyst, or officer), and at least one backup person should be trained.

Web site planners should take steps to see that the maps and data are used correctly and beneficially. It is prudent to define the

goals of the maps before creating them. If the goal is to give a general overview of crime throughout the jurisdiction, choropleth or other nonspecific address maps should be produced. Conversely, if a department wants to actively involve citizens in problem solving, different types of data and more specific (address or block level) maps may need to be released while still respecting the privacy of victims. In addition, the department should try to prevent an overreaction to specific crimes or crime problems and have a mechanism in place to respond to the community's questions and concerns about the maps and data. This response mechanism can be as straightforward as an e-mail address or contact person and number.

Mesa (Arizona) Police Department Interpretation Guidelines

NOTE: Throughout these reports, the term Calls For Service does NOT necessarily indicate a crime occurred—only that police interaction occurred.

Selected Calls for Service "Hot Spot" Density Map: A density map of the City of Mesa which is shaded to depict the areas within the city with the highest density of *selected* calls for service (CFS). The darkest shaded areas are the "hot spots" or areas with the highest density of CFS. Currently, this map depicts CFS for the fourth quarter of 2000.

Calls for Service Beat Maps: An interactive map of the city. First click on the desired area of the map. This enables you to point and click on specific beats within the city in order to view the calls for service that occurred in that specific beat.

Top 10 Intersections with Accidents: A list of the intersections with the most accidents. This list includes the most current information year-to-date, which is currently the fourth quarter of 2000. Also included are the top 10 lists for the entire year of 2000, the entire year of 1999, and the entire year of 1998.

Retrieved March 20, 2001, from the World Wide Web: http://www.ci.mesa.az.us/police/crime_analysis/patrol.htm.

Oakland (California) Police Department Interpretation Guidelines

Basic Statistical Concepts

Data means nothing without reference.

Time Frame - Are you comparing the same amount of time?

Location - Are you comparing the same area?

Data Definition - Are you comparing the same data elements? *CrimeWatch displays Crime Reports for a selection of Part 1 offenses. The dates you select by are the dates the crimes occurred.*

How did the environment change?

Time - Time frame this year compared with the same time frame last year. *Determine the total number of occurrences of a crime for a given time frame and find the change from last year.*

Excerpt from CrimeWatch GIS Instructions/ Tutorial. Retrieved March 20, 2001, from the World Wide Web: http://city.oakcc.com/maproom/statistics.html.

III. Maps on the Internet

Making crime maps available on the Internet is a big step. Before posting maps, an agency should consider a number of issues that may arise in the planning, implementation, and postimplementation stages. Some of the problems are technical, some are organizational, and some are related to effects on the community as a whole. If this is a department's first foray into putting information on the Internet, additional time and planning should be spent on broad Web-related issues.[28] There are numerous general concepts and questions not discussed here to be considered when providing information on the Web. These include authority, purpose, accuracy, timeliness, integrity of information, and viewpoint.[29]

Providing maps on the Internet can be cheap or expensive. If the maps are graphics (such as .jpg or .gif) and are updated monthly with a semiautomated process, the cost is only a few hours of staff time each month. By contrast, an interactive mapping system presents significant hardware, software, development, maintenance, and support costs. Oakland, California, spent $250,000 on a system implemented in 1999.[30]

Other concerns surround how the maps will be received, how they will be used, and what other effects they might have. The three major issues that law enforcement and the public have raised are the following:

- Potential for data misinterpretation and misuse.

- Victim privacy.

- Impact on property values and related "redlining" practices.[31]

The potential for misinterpretation and misuse of data by users is a valid concern. "Misinterpretation" means incorrectly understanding the map data and its implications; "misuse" means using the map data for an inappropriate purpose. Misinterpretation can occur if the maps are too complex or lead to assumptions based on a lack of understanding of statistics or crime data. For example, on a shaded map of crime rates in which the rate is determined by population (the most common denominator used), commercial areas of the city appear to have excessively high crime rates (see exhibit 2). Similarly, a shaded map may suggest that the entire area (e.g., beat, neighborhood) has a crime problem when in fact all the crimes are concentrated in one or two blocks within that area. For point maps, scale matters because a smaller scale may make crime look worse than it is.

Publicly available crime maps could, hypothetically, be misused (though the authors are not aware of any studies or official reports of misuse of publicly available crime maps). For example, alarm companies could target and bother residents on blocks or within neighborhoods that have high numbers of burglaries, or drug sellers and users could identify the "best" neighborhoods for their activities (by consulting a map of drug incidents, which would show where drugs are currently being sold). One means of possibly identifying misusers is to have everyone register and log on to the site. If there is any impropriety, the agency may be able to identify the user. Although this could be helpful in minimizing negative use, it may also limit or avert potential "good users" because of the additional step and the privacy sacrifice.

An agency can take several steps to reduce misinterpretation. If the Web site provides rates, it should also explain how
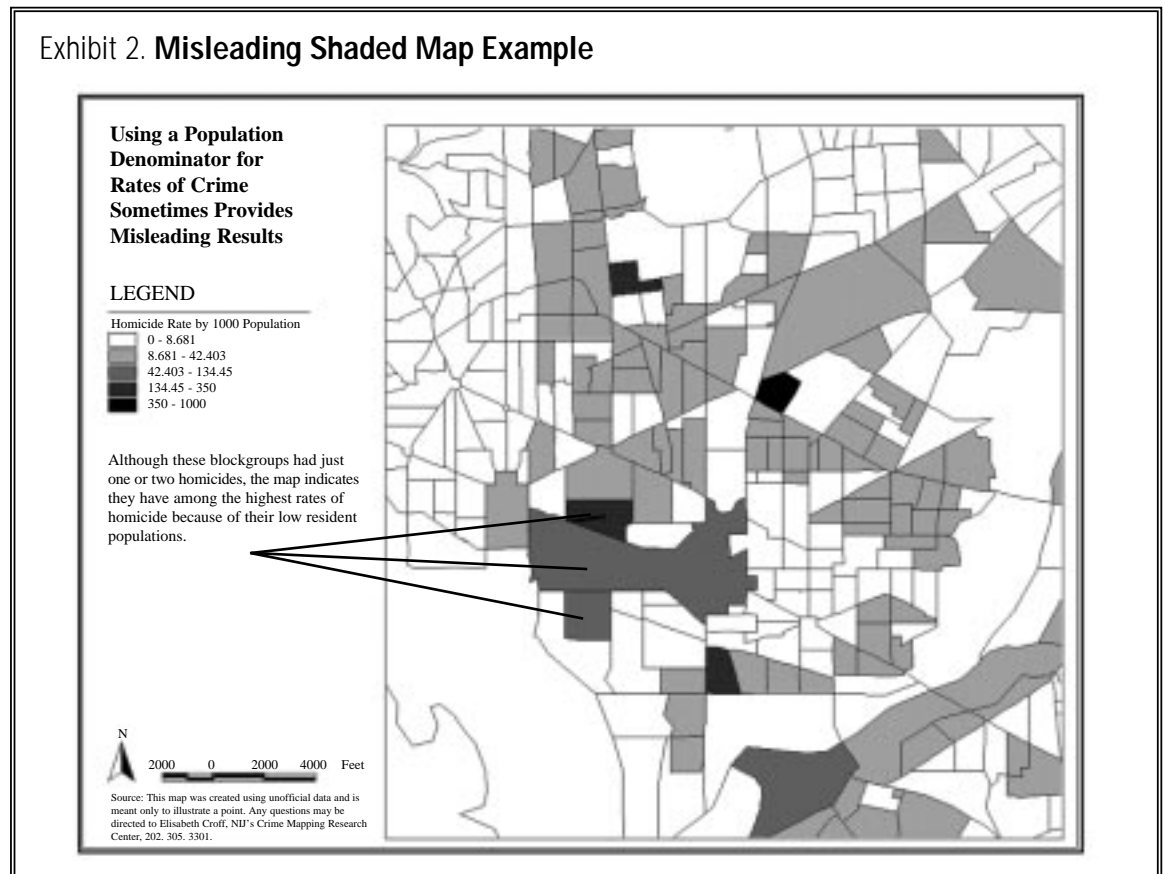
the rates were calculated and what they mean. Maps should show their scale so users can understand the significance of point density and estimate how far incidents are from their home or school. Site planners should avoid highly statistical or complex data and maps and should provide the data associated with each map. They also should keep in mind that if their agency does not provide crime maps and data to the public, others (such as the media or neighborhood groups) might—and they can interpret and display the information as they please.

Certain types of maps and data run the risk of violating victims' privacy by naming the exact location at which an offense occurred. As discussed in chapter 2, there is a concern that this can further traumatize a victim by revealing his or her identity. Some data are considered especially personal, such as data on sexual assaults; other data receive special legal protection, such as data on juvenile crimes. Shaded aggregate maps generally eliminate the ability to identify individual victims. Point maps can preserve privacy by plotting incidents on street centerlines (versus being offset for the side of the street or on a parcel). The level of map detail, scale, and symbol size can also obscure exact addresses. If the map point is clickable or if data tables are associated with it, address information should be limited to the 100 block. (See "San Diego County ARJIS" and exhibit 3.)

The notion that property buyers will use crime maps to avoid high-crime areas is primarily a supposition and has yet to be proven. In addition, naysayers of Internet crime mapping are quick to name redlining as a reason not to provide data. Redlining is a possibility, but it should not be the deciding factor. Even before crime maps were put on the Web, similar behavior occurred, for example, taxis avoided neighborhoods deemed dangerous.[32] A related concern is the potential for economic harm to businesses in crime-dense areas and the risk that insurance companies might raise rates.

Exhibit 2. **Misleading Shaded Map Example**

Using a Population Denominator for Rates of Crime Sometimes Provides Misleading Results

LEGEND

Homicide Rate by 1000 Population

- 0 - 8.681
- 8.681 - 42.403
- 42.403 - 134.45
- 134.45 - 350
- 350 - 1000

Although these blockgroups had just one or two homicides, the map indicates they have among the highest rates of homicide because of their low resident populations.

N

2000   0   2000   4000   Feet

Source: This map was created using unofficial data and is meant only to illustrate a point. Any questions may be directed to Elisabeth Croff, NIJ's Crime Mapping Research Center, 202. 305. 3301.

To date, however, no studies or evaluations have examined those theories. The opposing argument is that crime maps lead to greater public awareness of crime, which can promote community involvement in solving problems. In Tempe, Arizona, the police department posts crime statistics for its apartment communities, thereby creating competition among apartment managers to become involved in the Crime-Free Multihousing Program and improve their properties and rankings.[33] These types of maps can also be used to identify neighborhoods in need of additional resources.

To allay some of the fears listed above, agencies can refrain from placing statistics in order of best to worst or having individual neighborhoods stand out on a map. The latter can be avoided by grouping or categorizing areas instead of having 10 different shades for 10 different areas. It is especially important not to attach the terms "best" and "worst" to specific neighborhoods; instead, the site should let the numbers and maps speak for themselves. It may also be advantageous to work with area stakeholders, such as real estate agents, property management associations, and service providers (e.g., taxi and pizza delivery companies), by informing them that crime mapping data will be provided on the Web and obtaining their input on what would be useful and how they potentially would use the information.

Technical Approach

Certain technical decisions also need to be made. Web site planners should look at the following factors:

■ What data will be used (crime data versus calls for service, which crime types, what types of noncrime data)?

■ How will data be displayed on the map (points; aggregated by beat, census tract, or community; hot spots[34])?

Exhibit 3. **San Diego County ARJIS**
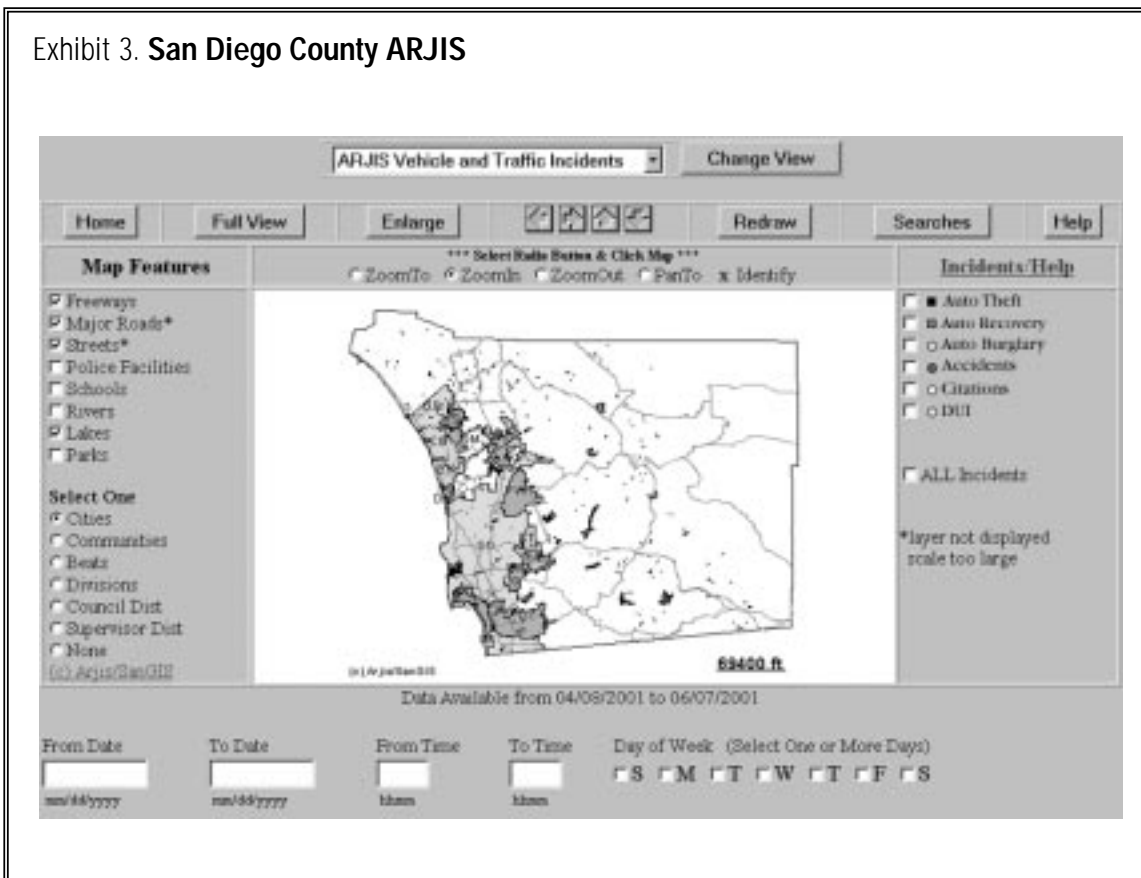
- How will the associated data tables or records be displayed (totals by area, listings, or individual records), and what information will be provided?

- Will users be able to make their own maps or see only what the department provides them (interactive versus static)?

- What types of general interpretation guidelines, explanations, and disclaimers will be given?

At the end of May 2000, the Crime Mapping Research Center knew of 38 Web sites that provided crime maps and data to the public.[35] Research for this chapter included a basic review of those sites.[36] Characteristics that were examined included data types, whether the maps were point or aggregate, what types of data tables were associated, whether map interpretation guidelines were provided, and whether a disclaimer was given. The results varied greatly in some categories and little in others. Of the 38 sites, 10 had maps without data; in other words, the maps had various boundaries (e.g., beats, neighborhoods, precincts), but the user had to click on the maps to get the associated data, which were in tabular format.

The 28 sites with mapped data primarily showed Part 1 or Index crimes. Some of the sites showed all Part 1 crimes; others selected four or five crimes to display. Most agencies used reported crime data, although some used calls for service. A few sites also had maps of sex offenders, drug incidents, vandalism, prostitution, and traffic accidents. Only a couple of sites gave

---

San Diego County ARJIS

By adopting the problem solving and community-oriented policing paradigm, the San Diego Police Department (SDPD) made a commitment to involve the community in its policing strategies. That commitment requires that the department disseminate information to the community. For nearly four years, SDPD provided static crime maps, listings, and statistics at its website. These data, representative of the previous month's crimes, were grouped into 101 neighborhoods.

Over time, the inadequacy of the static maps and the process for producing them became apparent. The primary complaints from community members, as well as department personnel, included the maps' lack of timeliness and relevance to community quality-of-life issues. In response, SDPD changed the update cycle from monthly to weekly; however the data still covered only the most recent 30 days.

With emerging "web enabled" GIS solutions, SDPD had to reassess what information should be provided, as well as how to provide an effective delivery mechanism. A collaborative effort between SDPD and the Automated Regional Justice Information System (ARJIS), a regional data repository of criminal justice information, allowed the development and implementation of a near real-time, publicly accessible crime mapping application known as ARJIS Interactive Mapping Application. Providing the application, which introduces greater user interaction with crime data, raised concerns over victim privacy. Those concerns were less evident when static maps were in use because the maps' scale precluded identification of victim addresses.

Privacy must be protected, but concern over privacy should not deter departments from providing the public with valuable information. In the case of ARJIS IMA, the data on crime, arrests, and citations (totaling 21 types of incidents) are not only extracted from ARJIS and the SDPD computer-aided dispatch (CAD) systems, but they are also filtered before being inserted into a geographic data warehouse independent of the source data. The majority of incident detail is stripped from each record, and the hundred-block address is provided as part of the interactive crime listing. Finally, these data overlay a limited number of geographic layers, such as schools, police facilities, and neighborhoods, while other layers (like San Diego parcels and Orthophotos) are not an option.

By Deena Bowman-Jamieson, Information Systems Analyst II, San Diego Police Department

arrest data. Several of the sites also provid-ed noncrime data, such as the location of schools, hospitals, and parks. Of the 28 sites, 21 displayed point maps, 3 showed aggregate maps by community, 2 had both point and aggregate maps (depending on the data type), 2 used only isopleth hot spot maps, and 1 had point and isopleth hot spot maps (see exhibit 4).

Only 7 of the 28 sites offered map interpre-tation guidelines, which often were limited. Several agencies noted that they did not have staff and resources to provide map interpretation. Twelve had disclaimers, and several more had definitions or expla-nations of the crime types and data. Examples of the latter include how the statistics were derived and the source of the information.

Just 4 of all 38 sites examined did not have statistics either directly associated with the maps or elsewhere on the Web site. The data and statistics were displayed in numerous ways and updated on different schedules, but the majority included Part 1 crimes totaled by census tract, neighborhood, beat, or city. Several of the sites had crime or

traffic listings or the ability to identify the points or query results. Of these, some used the 100 block for the address or did not list an address (only date, time, and reporting area). In addition to Part 1 crimes, a few sites included other crime statistics, such as selected call types, sex offenders, traffic incidents, and Part 2 crimes.[37] Several agencies allow the public to download statistical tables.

Most of the 38 Web sites were created by law enforcement agencies. The remaining four were run by a university, a newspaper, a television station, and another independ-ent company. Of the 28 sites with maps, only 7 used interactive mapping in which the user could select criteria such as crime type, date range, or area. The interactive sites ranged in functionality and output, and some included "help" files. The static maps (unchangeable graphics put on the Web site by the agency) varied greatly in the time-frame of data presented and in the frequen-cy in which they were updated (weekly, monthly, or yearly). Although more agen-cies published their maps and statistics in a central location on the Web site (such as crime analysis), some were associated with community or patrol area pages. Maps can be published on the Internet in many different ways; the best approach is to plan carefully and make the most of the agency's technical and staff resources.

Essentially, an agency needs a server to house the data, a spa-tial engine, and the front-end application. Several companies sell the software necessary to put interactive maps on the Web.[38] Prices and functionality vary widely, and GIS, network, programming, and law enforce-ment experts should be involved in selecting products. Once the appropriate mapping software is in place, a means needs to be developed to obtain the data, geocode them if necessary, and modify the addresses (so the

Exhibit 4. Types of Maps on the Internet

Number of Web Sites With Maps

Types of Maps
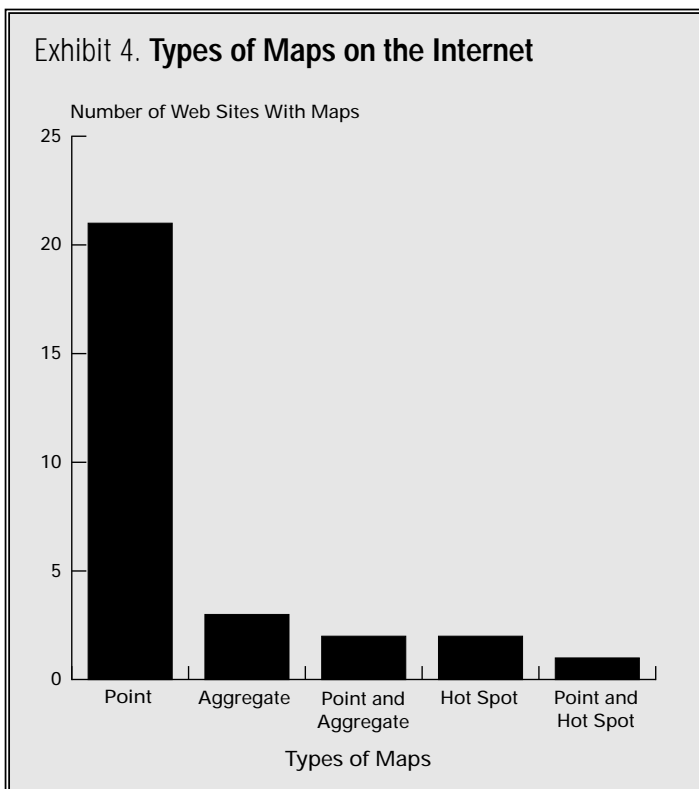
exact addresses are not identifiable to the public) on a regular basis.

Security Issues

When putting maps on the Internet, an agency must be aware of site and data security. Maps available to the public on the Internet generally are not access controlled. An exception may occur if police departments want to provide particular groups, such as neighborhood watch associations, with detailed maps on crime in their areas but not make those same maps available to anyone else. In such a case, the police department should establish some means of security, such as the use of passwords or encryption.

Data security issues are virtually nonexistent for static maps. These maps are graphical images, and the data behind them are not accessible. The real concern is privacy, not security. Data security, however, is an issue for interactive crime maps, especially if they use point data. The potential for hackers to access police records through the department's Web site is a real concern. To secure the data behind interactive maps, departments could use some or all of the following techniques:

■ Establish a firewall to protect the entire Web site.

■ Use a separate server or database for the Internet data and maps (a copy of the records management system or computer-aided dispatch that department personnel access internally).

■ Do not include victims' names or exact addresses.

■ Use security-checking software.

Departments that currently post interactive crime maps on the Internet have dealt with security issues in different ways. Considerations include the source of the data, the information contained in the data, other information on the Web site, and the level of paranoia (or caution) of programmers and management. The best approach is to talk with people who have already secured law enforcement Web sites. Security clearly must be tackled in the planning process, not after there has been a breach. See appendix B for further security information and resources.

IV. Sharing Data With Other Agencies

As observed in chapter 1, diverse datasets can now be merged more easily than in the past. This linking of data may be across units within a department (gang information and traffic warrants), across departments within a city (police and zoning), or with other law enforcement agencies. The data sharing may be organized through partnerships between neighboring law enforcement agencies, between local police and State corrections, or through a regional community safety concept of law enforcement, prosecution, education, and health. (See "Winston-Salem Community Safety Information System" and exhibit 5.)

In a data-sharing partnership, the greatest challenge often arises not from data or technology but from the politics and personalities of the agencies. However, with common goals and a willingness to share, the logistical aspects can run smoothly. Currently, several data-sharing programs are under way, sharing police and other government data (both GIS related and nonspatial) across agencies and jurisdictions.[39]

Exhibit 5. **Winston-Salem Community Safety Information System**
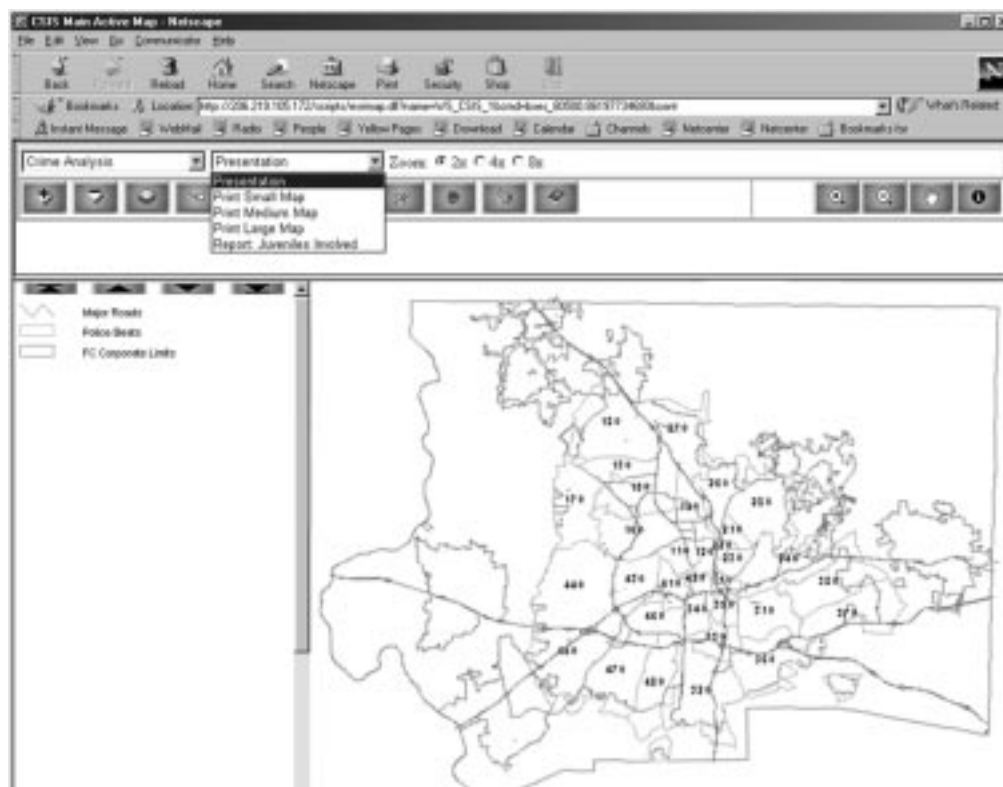
In Orange County, California, a cross-jurisdictional gang-tracking system was developed in 1993. A local university maintains the system, but the data are owned by the individual agencies. Maps and other products cannot be shared across agencies or outside the county without each chief's permission. In the Baltimore, Maryland, metropolitan area, the Regional Crime Analysis Geographic Information System was recently created for 13 city and county law enforcement agencies to share an application and its associated crime maps and data. All agencies involved agreed several years ago, when a regional crime analysis (non-GIS) system was developed, that a cross-jurisdictional database would be much more effective for solving and reducing crime.

In its 1999 report "Making the Best Use of Government Data," the New York Area Data Council provides a number of recommendations to increase data sharing.[40] There are pros and cons to all of these recommendations, and each should be considered as to its effect on privacy rights.

1. Executive offices of government at all levels should establish firm policies in favor of data sharing. They should increase public servants' awareness that data collected for agency needs are likely to have value to other organizations performing different functions.

2. Public policy should promote cooperation among agencies, public and private, in data collection, maintenance, and interchange.

3. State legislatures should foster the data sharing process with guidelines that promote (a) public acknowledgment of the data source and its ownership and (b) cooperative relations between data users and providers.

4. Regional data are difficult to gather where there is no regional government presence. Regional indicators assist planning and other important government decisions, and the collective data must come from somewhere. An organization such as the New York Metropolitan Transportation Council should be financed to collect data of economic and social interest at the tri-state regional scale.

5. Within the broad principle of making data widely and easily available, privacy and secrecy must be protected. Individuals should have the right to legal recourse when their privacy has

---

Winston-Salem Community Safety Information System

The Winston-Salem Community Safety Information System (CSIS) grew out of a Department of Justice project called Strategic Approaches to Community Safety Initiative (SACSI). Winston-Salem was one of three sites that received funding and technical assistance to create a regional, cross-discipline geographic information system application to attack community safety problems.

CSIS is accessible via the police department's intranet and via Internet with a password protected login or with a guest login that has very limited capabilities. The guest login allows viewing of data layers with no querying or analysis capability. Only demographics, roads, jurisdictions, police patrol areas, other non-crime data, and select crime layers are available to non-privileged users. Those layers include current motor vehicle theft and recovery locations, house and store break-ins, robberies, assaults with firearms, and drug violations. No victim or suspect details are available. Site users can gain a geographic overview of crime locations relative to other environmental factors, yet an individual's privacy remains protected.

The school system has expressed concern about confidentiality and has only provided aggregated discipline and attendance data by schools. No student names or demographics are available.

Names in the offense and arrest data are accessible to users with a login and password. Home addresses of arrestees and offenders are also available.

By Julia Conley, Senior Systems Analyst, Winston-Salem Police Department

been violated, including the right to correct false information. Legislatures should set policy, and agencies should be held responsible for carrying out that policy.

6. Useful data can often be provided without violating secrecy and privacy if it is suitably aggregated or summarized.

7. Agency heads and budget offices should recognize that data collection and maintenance are integral components of many public agency goals and should fund them consistently.

8. Public offices should assure professional standards in data handling. High-quality, dependable data, free of wrongful disclosure, require that.

9. Data-collecting agencies should provide a full description of data (metadata) with distribution. Metadata should detail data encoding, data gathering, and sources of error.

10. Providing data is useful only if prospective users know the data are available. Governments should use all forms of publicity to accomplish this.

11. Data distribution format is important in facilitating its use, especially by organizations that do not have highly professional research capacity. Governments should provide information on paper as well as in electronic form, laid out so it is easy to understand and analyze.

12. Data users have a responsibility to data providers. They must acknowledge the source, sending to the data source research based on data provided, commenting to the source on the accuracy and clarity of the data, and most importantly, using data with care to avoid misinterpretation.

13. Recognizing that there are costs to making data usable and widely available, users might legitimately be asked to pay the full marginal cost, especially if the users will profit from the data. However, government data should be available to the public free of charge

where it is essential to assure responsive and responsible government.

14. Some issues should be clarified by further public debate, such as the question of when market pricing may be appropriate, how to safeguard privacy interests, and what recourse individuals have when their privacy is violated.

The first step in determining what information can be shared is to become familiar with applicable State and Federal laws. Public records and privacy laws vary greatly by State but are typically specific about the disclosure of incident, crime, and arrest information. (See "California Public Records Act Government Code 6250–6270" for one example of a State law.) James Meeker, a professor at the University of California, Irvine, observes, "Since the law places no limits on what may be done with public information, it follows that law enforcement agencies are not responsible for misuse of public information that they are required by law to release."[41]

One manner of misuse of information, according to a recent U.S. Supreme Court decision, is the dissemination of police record information solely for commercial purposes. In December 1999, the Supreme Court in *Los Angeles Police Department* v. *United Reporting Publishing Corp.*, upheld California Government Code 6254 (amended July 1996), which limits public access to the addresses of crime victims as well as those arrested for committing crimes. The Freedom Forum notes, "Under the law, anyone seeking names and addresses of arrestees and crime victims must certify that they will use it for journalistic, scholarly or governmental purposes, and not for the sale of a product or service. The law was ostensibly aimed at protecting the privacy of crime victims."[42]

Although jurisdictions have enacted laws and policies regarding the distribution of individual or tabular criminal history, incident, arrest, and traffic records, the laws do not speak specifically to geocoded data and maps. When providing geocoded data

and maps to other agencies, an agency should consider doing the following:

1. Provide the information in compliance with State laws regarding liability, freedom of information, and privacy.

2. Provide contact information of persons with expertise in those matters and familiarity with the data.

California Public Records Act Government Code 6250–6270

6254 (f) requires that State and local law enforcement agencies shall make public:

Subsection (1)

- Full name and occupation of every individual arrested by the agency,

- Individual's physical description,

- Time and date of booking,

- Location of the arrest,

- Factual circumstances surrounding the arrest,

- Amount of bail set, time and manner of release, or the location where the individual is currently being held, and

- All charges the individual is being held upon, including any outstanding warrants from other jurisdictions and parole or probation holds.

Subsection (2)

- Time, substance, and location of all complaints or requests for assistance received by the agency and the time and nature of the response thereto, including, to the extent the information regarding crimes alleged or committed or any other incident investigated is recorded, the time, date, and location of occurrence,

- Time and date of the report,

- Name and age of the victim,

- Factual circumstances surrounding the crime or incident, and

- General description of any injuries, property, or weapons involved.

---

3. Discuss whether the data provided will be merged with other data; if so, consider whether the combined files create privacy or other problems.

Data Clearinghouses and Standards

Currently, there are two major resources for criminal justice and spatial data. The National Archive of Criminal Justice Data (NACJD), a branch of the Inter-university Consortium for Political and Social Research at the University of Michigan, acquires, archives, processes, and provides access to computer-readable criminal justice data collections for research and instruction.[43] These collections include data from projects from various agencies, including the Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, Federal Bureau of Investigation, U.S. Sentencing Commission, Federal Judicial Center, and Urban Institute. Although NACJD provides free, downloadable access to more than 500 criminal justice data collections, few contain spatial data.

The other major resource is the National Spatial Data Infrastructure (NSDI), created by Presidential Executive Order in 1994. NSDI is coordinated by the Federal Geographic Data Committee and is made up of 17 Federal agencies.[44] NSDI's goal is to promote consistent access and sharing of geographic information by providing spatial data, standards, metadata, and clearinghouses to the public. NSDI is constantly evolving through a series of strategic partnerships and input from organizations in State, local, and tribal governments; academia; and the private sector, including Federal agencies, State geo-information councils, the National States Geographic Information Council, the National Association of Counties, the National League of Cities, universities (through the University Consortium for Geographic Information Science), the Open GIS Consortium, and ecological and conservation groups.[45]

Through an infrastructure for managing spatial data, NSDI serves as a resource for several organizations in the environmental, health, geology, ecology, transportation, and planning fields. Although NSDI contains no law enforcement or criminal justice data,[46] structurally and organizationally it could. Currently, there are more than 200 spatial data servers in the National Geospatial Data Clearinghouse, a component of NSDI.

Any agency or member of the public can use this digital geographic data by using the Web interface to search on a variety of metadata fields. NSDI uses the national metadata standards to ensure an accurate inventory and search capabilities. In addition, NSDI uses several mechanisms to advertise the data's existence while still safeguarding its content.

V. Sharing Data With Researchers

Police departments have long provided researchers with crime data. Because most of the data were in the public record, doing so posed no privacy risks. Aggregate data rather than individual records sometimes were provided. The difference now is that geocoded data, while still technically in the public record, provide more precise information than data previously given to researchers. Examples include addresses of victims, known gang members, and arrestees. This precision should not prevent agencies from sharing geocoded data, but it should encourage departments to use extra caution in providing such data. Another publication that discusses similar issues is *A Question of Balance: Private Rights and the Public Interest in Scientific and Technical Databases.*[47] In this report, the Committee for a Study on Promoting Access to Scientific and Technical Data for the Public Interest examines the concerns regarding balancing the rights of database producers with "downstream" users such as researchers, educators, and librarians.

Data sharing between law enforcement agencies and researchers can benefit both parties. Before data are exchanged, both parties should discuss what data will be released, in what format, whether the researchers will have direct access to the data, how long the project will last, how the data will be used, how data will be secured or destroyed, and the potential consequences of the findings.

Whereas data sharing used to mean providing hardcopy reports with the names blacked out, it now usually means providing electronic tables or spreadsheets with identifying information deleted. With the advent of GIS, specific address data have increased greatly in value. Researchers have analyzed cities, neighborhoods, and census tracts for years. Now they want to be as specific as possible, both to test theories as well as to help police reduce crime and make neighborhoods safer.

Hartford, Connecticut, provides a unique example of sharing raw data with a researcher and the community (see "Neighborhood Crime Mapping in Hartford.") The police department and a community organization had simultaneously started to think about sharing crime data, then a researcher was able to make it a reality. Although some believed the community would use the information as a basis for criticism of the department, the chief and others felt it should be released. The community wanted as much information as possible, while the department was concerned about privacy and confidentiality. Serving as an intermediary, Tom Rich, the researcher from Abt Associates, was able to get the two sides to agree on what information would be released and how users could get it. There was no written data-sharing agreement. Rich believes that although his well-established relationship with the police department made it easier to create the partnership, basing the process on a research project (that came to an end) may have hindered the institutionalization of data sharing.

Guiding Principles

Certain law enforcement agencies have continuously opened their doors to researchers, and certain researchers have often been invited to study various aspects of a department. These partnerships, some more extensive than others, have benefited the policing field.

In some projects, the department provides the researcher with data on which to perform further analysis. For example, in San Diego, a unit in the police department began examining the prescription fraud problem. The detectives had collected some data, performed minimal analysis, and created a few maps. Because the department lacked the resources to produce extended analysis and summaries, it provided the geocoded and nonspatial data to several researchers.[48]

Neighborhood Crime Mapping in Hartford

During the mid-1990s, a Hartford Comprehensive Communities Partnership needs assessment identified access to computerized police databases as one of the most critical information requirements for effective problem solving. While departments across the country were improving information accessibility in a number of ways, Hartford chose to provide community organizations with raw data and its own mapping and analysis tools.

With funding from the National Institute of Justice, a project was started in which community organizations received raw data on calls for service, crime, and arrests—through the grant researcher—to map and analyze on their own with custom mapping software. None of the data contained names; arrest data contained specific addresses, while calls and incidents were identified by 100 blocks. The data were sent already geocoded with x,y coordinates.

This data-sharing partnership between the police department, the researcher, and the community organization is considered a success. The Hartford city manager, police chief, and other police managers have been greatly supportive, and the community has not only been appreciative but also become actively involved in community policing.

Information taken from Crime Mapping Case Studies: Success in the Field *(Rich, 1998) and June 13, 2000, phone interview with the researcher, Tom Rich.*

At the other end of the spectrum are long-term, ongoing studies in which a researcher works side by side with law enforcement or other criminal justice agencies. Two National Institute of Justice-funded projects exemplify this type of partnership. Boston's gun violence reduction project, led by David Kennedy and a team from the Kennedy School of Government at Harvard University, worked closely with the police and probation departments to analyze and strategically respond to the juvenile gun violence epidemic.[49] The New York City Police Department has also enjoyed an excellent partnership with geographic researchers from Hunter College of the City University of New York. The researchers are permitted to use real police data to test their theories, while the department gains research and tools to assist in operational policing. Similar partnerships are described in a January 1999 *National Institute of Justice Journal* article called "NIJ's Locally Initiated Research Partnerships in Policing—Factors That Add up to Success."[50]

During CMRC's Crime Mapping and Data Confidentiality Roundtable, two experts—a researcher and a police practitioner—were asked about the requirements for a successful police-researcher data-sharing partnership. Andreas Olligshlaeger of Carnegie Mellon University suggested that agencies use the following general guidelines when providing data to a researcher:[51]

1. Determine the type, format, and nature of the data required to do the research. The researchers and the agency should work together to decide what data will be needed. Data sensitivity should be considered for both the raw data and the results. A nondisclosure agreement may be used to guarantee confidentiality.

2. Decide how the results of the research will be presented. Some data might appropriately be shown at the address level, while other data may need to be aggregated before being published. Considerations include the privacy of individuals as well as the sensitivity of certain law enforcement information. The agency should have a chance to review any research results before publication.

3. Perform background checks on research personnel who will have access to data. Some agencies do this; others may not.

4. Decide where data will be stored. Sensitive or restricted data should always be kept on secure servers. If the researcher does not have secure storage (as is the case at many universities), one option is to have the researcher work on the law enforcement agency's system.

5. Require researchers to destroy raw data after the research is completed. Researchers often overlook this step. Even if the data are stored on a secure system, computers get replaced, and it is easy to forget after a few years that the data are still there.

Dennis Nowicki, former chief of the Charlotte-Mecklenburg Police Department in North Carolina, suggests the following questions should be asked when a researcher requests data or asks to partner with a police department:[52]

1. Does the research add value to the policing profession, to the community, or to society . . . [in general]?

2. Are the researcher's capabilities and integrity acceptable?

3. Will the department be given feedback throughout the data-gathering stage? Are the results or findings likely to surprise the department?

4. Can the researcher guarantee that the data will be used only for the agreed-upon research purpose? Will personal identities be kept confidential?

5. Will the researcher agree to regular meetings with police personnel to discuss the project, including the interpretation of data analysis and maps? Will the researcher agree to involve the department in reviewing the final report?[53]

Every research project is different, and the uses and products vary greatly. But these suggestions can lead to greater consistency, fewer problems, and a better basis for supporting future data-sharing partnerships. Potential partners may also want to consider writing a memorandum of understanding (MOU) regarding the use of the data, findings, and the overall research project. The MOU should include answers to the above-mentioned questions and issues.

Agencies also must take care to consult laws and regulations governing the sharing of data with researchers. Many State laws regarding privacy, confidentiality, and release of public records apply to the public, other agencies, and researchers. If the research is conducted through a Federal grant, additional rules and regulations apply. These include the protection of human subjects,[54] privacy certificates, and confidentiality requirements.

Conclusion

The sharing of mapped information among law enforcement agencies, the public, and researchers is in place, but many issues have yet to be resolved. The reality, as reflected in this report, is that many agencies have moved forward with decisions on what data should be available through maps, how that data will be displayed, what the agency should provide as a disclaimer, and how to make data available to others. A goal of this report has been to summarize what currently exists in these areas.

Of particular note is that law enforcement agencies generally have favored making crime and other data available in a mapped format while at the same time remaining sensitive to the privacy of victims. A general conclusion by an increasing number of people is that the public's desire for mapped data can be honored without compromising privacy and other issues. As noted in this report, several agencies are using the Internet as a means of displaying mapped data.

It will remain important for law enforcement agencies to make sound decisions on several issues as maps are made available. Agencies must decide exactly what data they want to display; they must develop a disclaimer for consumers; they must stay within the provisions of their State laws regarding privacy of addresses, phone numbers, and other information; and they must provide guidelines to consumers on how to interpret maps. There are also technical issues to be addressed. Foremost is whether the maps will be available on the Internet and, if so, whether they will be interactive or static. Technical considerations, such as map symbols, map scale, and legend must be addressed.

The sharing of mapped data with other government agencies and with researchers involves all the considerations previously mentioned and introduces others. In these instances, entire datasets may be provided, rather than only the final mapped products. Consequently, agreements should be developed between agencies on what data will be provided, how others will use the data, and whether preparation costs will be shared. Several agencies have found positive benefits in developing partnerships with researchers. As noted, researchers in Hartford, Boston, Charlotte, and elsewhere have successfully teamed with their local police agencies on mapping projects with positive results. These partnerships must be formed carefully (as discussed in this report) but if they are properly established, they can be beneficial to both parties.

The goal of this report is to assist agencies that are interested in sharing data and maps to become more knowledgeable about the issues. Oftentimes, standards have not been well received in local law enforcement; therefore we have provided this guide which we hope will be much more acceptable as more agencies begin and continue to explore this field. This guide should be used to assist in planning and implementation, but it should not be used without careful consideration of individual jurisdictions and situations. "What data to present" will vary according to the needs, capabilities, and environment of the jurisdiction. Other information, such as the use of disclaimers, geocoding rates, interpretation, and the correct and current use of maps and data, is more general and straightforward. Finally, an evaluation of what is currently being done and the obstacles those agencies have faced should be used in conjunction with any guidance that is followed.

Crime mapping is still considered a relatively new field. The use of the Internet is also a new and emerging area. Combining these two practices has shown great opportunity, but the field must use caution on how these data and technology are applied. In addition, there is a strong push for sharing data across agencies and with researchers. Although these are also significant advances, implementing this data sharing and public access should not be conducted haphazardly. Agencies should do extensive planning, gather input from all stakeholders, and examine how others have already implemented these practices. This report examined a number of concerns and offered a variety of guides, but in truth, there are still many unresolved issues and a need for further exploration and evaluation.

Notes

1. See appendix C, Glossary, for definition and explanation of terms.

2. This access included various forms of distribution, not solely the Internet. More specific data regarding citizen access to crime statistics can be found in the complete report, Reaves, Brian A., and Andrew L. Goldberg, *Local Police Departments 1997*. Washington, D.C.: U.S. Department of Justice, Bureau of Justice Statistics, February 2000, NCJ 173429.

3. Lake, David, "It's a Web World, After All," *The Standard*, December 18, 2000. Retrieved March 14, 2001, from the World Wide Web: *http://www.thestandard.com/article/display/0,1151,20915,00.html.*

4. Survey conducted by the Crime Mapping Research Center in 1997. See Mamalian, Cynthia A., Nancy G. La Vigne, and the staff of the Crime Mapping Research Center. *The Use of Computerized Crime Mapping by Law Enforcement: Survey Results.* Research Preview, Washington, D.C.: U.S. Department of Justice, National Institute of Justice, January 1999, FS 000237.

5. Ellard, Timothy, "Public Attitudes Toward Uses of Criminal History Information," SEARCH National Conference on Privacy,

Technology, and CJ Information, May 31, 2000. Retrieved June 15, 2000, from the World Wide Web: *http://www.search.org/conferences/priv_tech_2000/Agenda.htm.*

6. The U.S. Department of Education recently started a Web site *(http://ope.ed.gov/security)* on which crime statistics are available for all colleges and universities, which are now required by law to report annual data.

7. The paragraph below each numbered item contains the issues discussed by participants at the NIJ Crime Mapping and Data Confidentiality Roundtable, CMRC, Washington, D.C., July 8–9, 1999.

8. More information about the Freedom of Information Act can be found at *http://foia.fbi.gov.*

9. Vila, Bryan, "Privacy: Can We Achieve It? Should We Even Try?" Presentation given at the National Institute of Justice Crime Mapping Research Center International Conference, Orlando, FL, December 14, 1999.

10. Boba, Rachel, "Using the Internet to Disseminate Crime Information," *FBI Law Enforcement Bulletin* 68 (10) (October 1999): 6.

11. CMRC list serv posting by George Tita, Carnegie Mellon/RAND, January 12, 1999.

12. CMRC list serv posting by Spencer Chainey, formerly the GIS manager at the London Borough of Hackney, January 7, 1999.

13. For an indepth discussion of cross-jurisdictional crime mapping, see the forthcoming Police Executive Research Forum/National Institute of Justice publication, Lavigne, Nancy G., and Julie Wartell "Mapping Across Boundaries: Regional Crime Analysis."

14. Although there is no proof that this occurs, it could be the basis for a large-scale evaluation of offenders' habits.

15. This information was gathered from CMRC list serv postings and several Web

sites. For information about German policy, see *http://www.brandenburg.de/land/mi/sitemap.htm* (in German). For information about United Kingdom policy, see *http://www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm* and *http://www.homeoffice.gov.uk/cdact/actgch5.htm.*

16. Thornburg, Ryan, "GIS and the Privacy Puzzle," *Governing* 13 (3) (December 1999): 60–61.

17. Hammitt, Harry, "Personal Issues: Courts Wrestle with What to Post," *Government Technology* 13 (4) (March 2000): 62.

18. A summary of Megan's Law (found at *http://thomas.loc.gov/cgibin/bdquery/z?d104:HR02137:@@@L&summ2=m&ITOM:/bss/d104query.html)* states: "(1) require . . . State and local law enforcement agencies to release relevant information that is necessary to protect the public concerning persons required to register under a State registration program established under the Jacob Wetterling Crimes Against Children and Sexually Violent Offender Registration Act; and (2) provide that any information collected under such a program may be disclosed for any purpose permitted under the laws of the State."

19. See memorandum M99–18 from Director Jacob J. Lew, Office of Management and Budget to all Heads of Executive Departments and Agencies. Retrieved March 20, 2001, from the World Wide Web: *http://www.whitehouse.gov/OMB/memoranda/m99-18.html.*

20. See the U.S. Census Bureau Web site at *http://www.census.gov/main/www/policies.html.*

21. See the National Archive of Criminal Justice Data Web site at *http://www.icpsr.umich.edu/NACJD/privacy.html.*

22. For further explanation, see CMRC's training module, *What is Crime Mapping?*, at *http://www.ojp.usdoj.gov/cmrc/training/download.html.*

23. Casady, Tom, "Privacy Issues in the Presentation of Geocoded Data," *Crime Mapping News* 1 (3) (Summer 1999): 2.

24. The Federal Bureau of Investigation's Uniform Crime Reporting Program lists the eight Part 1 or Index crimes as murder, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson.

25. For higher numbers of incidents, larger, darker color symbols of the same shape are frequently used.

26. For example, see the Sacramento Police Department's Web site at *http://www.sacpd.org.*

27. This is an estimate based on the FBI's 1999 Uniform Crime Reports and is only being used for illustrative purposes.

28. For specifics on Internet issues for criminal justice, see *The Definitive Guide to Criminal Justice and Criminology on the World Wide Web* (Criminal Justice Distance Learning Consortium, 1999) and *Rookie's Guide to Creating WebSites* (Wilson, 1998).

29. These concepts are expanded on at *http://libweb.sonoma.edu/web/eval.html.* Also see Hammett, Paula, "Teaching Tools for Evaluating World Wide Web Resources," *Teaching Sociology* 27 (1) (January 1999): 31–37.

30. Chen, Hans, "Cops Put Crime Maps Online," APBNews, January 3, 2000. Retrieved January 5, 2000, from the World Wide Web: *http://www.apbnews.com/cjprofessionals/behindthebadge/2000/01/03/crimemap0103-a.html.*

31. Redlining refers to the practice by banks of not providing loans based on the knowledge of crime in a neighborhood. Neighborhoods that have been subjected to redlining in the past often had a high percentage of minorities.

32. Although Domino's Pizza won a racial bias suit in October 2000 after refusing to deliver to specific parts of some neighborhoods, the company's new delivery policy, created in June 2000, "ensures that decisions on delivery limitations will be based on the legitimate concern for the safety of Domino's employees and not on the racial composition of a neighborhood" (Bill Lann Lee, Acting Assistant Attorney General for

Civil Rights in Sniffen, Michael, "Domino's resolves bias claim by changing delivery policy," *Seattle Times* Web site, June 6, 2000. Retrieved March 20, 2001, from the World Wide Web: *http://seattletimes. nwsource.com/news/nation-world/html98/ pizz06_20000606.html.* The new guidelines require that store owners and managers evaluate crime statistics with local law enforcement agencies and community groups before limiting delivery. See Zuber, Amy, "Pizza 'redlining' accord may have domino effect," *Nation's Restaurant News*, FindArticles.com, June 19, 2000. Retrieved December 1, 2000, from the World Wide Web: *http://wwwfindarticles.com/cf_0/ m3190/25_341/62990475/print.jhtml.*

33. Boba, "Using the Internet to Disseminate Crime Information."

34. In this instance, "hot spots" means smoothed (not aggregated to a specific boundary) crime concentrations.

35. An updated list can be viewed at *http://www.ojp.usdoj.gov/cmrc/weblinks/ welcome.html.*

36. This review looked only at the various approaches to putting the data and maps on the Internet; it did not include quality or effectiveness measures.

37. Part 2 crimes include but are not limited to drunk driving, weapon violations, vandalism, disorderly conduct, drug crimes, fraud, and obscene phone calls.

38. See the list on the CMRC Web site, *http://www.ojp.usdoj.gov/cmrc/weblinks/ welcome.html.*

39. For five case studies, see *Mapping Across Boundaries: Regional Crime Analysis*, forthcoming from the Police Executive Research Forum.

40. Some of the recommendations are specific to the New York area but could easily be adapted to any jurisdiction. For a copy of the summary and complete report, go to *http://web.gc.cuny.edu/cur/Frames/ home2.htm,* click on "New York Area Data Council," then select "New York Area Data Council Reports."

41. Meeker, James, "Accountability for Inappropriate Use of Crime Maps and the Sharing of Inaccurate Data," "Crime Mapping and Data Confidentiality Roundtable Notes," CMRC, July 1999. Retrieved February, 2001 from the World Wide Web: *http:// www.ojp.usdoj.gov/cmrc/pubs/privacy/ meeker.pdf.*

42. Mauro, Tony, "Supreme Court backs limits on police blotter data." The Freedom Forum, December 7, 1999. Retrieved March 22, 2001, from the World Wide Web: *http://www.freedomforum.org/templates/ document.asp?documentID=10334.*

43. For more about NACJD, see *http://www. icpsr.umich.edu/NACJD/welcome.html.*

44. For more about the Federal Geographic Data Committee and NSDI, see *http:// www.fgdc.gov.*

45. Nebert, Doug, and Mark Reichardt, "Managing Confidentiality: Building Blocks for Protection and Access of Health Information," CDC, February 15, 2000. Retrieved June 21, 2000, from the World Wide Web: *http://www.fgdc.gov/publications/documents/ ppt/powerpoint.html.*

46. In September 2000, a search of "crime" on about 20 spatial data servers came up with zero results.

47. National Research Council. *A Question of Balance: Private Rights and the Public Interest in Scientific and Technical Databases*. Washington, DC: National Academy Press, 1999.

48. Nancy La Vigne, Office of Justice Programs, and Julie Wartell, Institute for Law and Justice, presented preliminary results from this project at the American Society of Criminology Conference in November 2000.

49. For more on this gun violence reduction project, see *http://www.ncjrs.org/txtfiles/ boston.txt.*

50. McEwen, Tom, "NIJ's Locally Initiated Research Partnerships in Policing-Factors That Add up to Success," *National Institute of Justice Journal* 238 (January 1999): 2–10. The article is available online at *http://www.ojp.usdoj.gov/nij/journals/jr000238.htm.*

51. Andreas Olligschlaeger developed the five guidelines in a paper written for the CMRC Roundtable. Some of the explanations have been paraphrased.

52. These questions are extracted from the CMRC Roundtable Notes (CMRC, 1999).

53. The intent of this review would be to inform and correct factual errors, not to bring in the opinion of the department to alter any results.

54. See NIJ's Protection of Human Subjects (regulations) at *http://www.ojp.usdoj.gov/nij/humansubjects/hs_02.html.*

Resources

28 C.F.R. Part 22. *Confidentiality of Identifiable Research and Statistical Information.*

28 C.F.R. Part 46. *Protection of Human Subjects.*

42 U.S.C. Section 3789g. *Confidentiality of Information.*

APB News Online, Web site: *http://www. apbnews.com.*

Block, Carolyn Rebecca, "STAC Hot Spot Areas: A Statistical Tool for Law Enforcement Decisions," in *Crime Analysis Through Computer Mapping,* ed., C.R. Block, M. Dabdoub, and S. Fregly, Washington, DC: Police Executive Research Forum, 1995.

Cheetham, Robert, "Data Sharing, Security and the Internet," Presentation given at the Crime Mapping and Data Confidentiality Roundtable, Washington, DC, July 9, 1994.

Crime Mapping Research Center (CMRC), "Crime Mapping and Data Confidentiality Roundtable Notes," CMRC, July 1999. Retrieved February 2001 from the World Wide Web: *http://www.ojp.usdoj.gov/ cmrc/pubs/privacy/privacy.html.*

Crime Mapping Research Center, CRIMEMAP list serv postings, December 17, 1998, to January 12, 1999.

Crime Mapping Research Center, Web site: *http://www.ojp.usdoj.gov/cmrc.*

Criminal Justice Distance Learning Consortium, *The Definitive Guide to Criminal Justice and Criminology on the World Wide Web,* Upper Saddle River, NJ: Prentice Hall, 1999. Retrieved February 2001 from the World Wide Web: *http://talkjustice.com/files/ guide.htm.*

Electronic Privacy Information Center, Web site: *http://www.epic.org.*

Freedom of Information Act Guide, May 2000. Retrieved March 15, 2001, from the World Wide Web: *http://www.usdoj.gov/ oip/foi-act.htm.*

Goodman, Marc, "Working the 'Net." *Police Chief* (August 1997): 45–53.

Greenman, Catherine, "Turning a Map into a Layer Cake of Information," *New York Times,* January 20, 2000.

Lubove, Seth, "Redlining Software," *Forbes* April 5, 1999. Retrieved May 14 2000 from the World Wide Web: *http:// www.forbes.com/forbes/1999/0405/ 6307053a.html.*

National Archive of Criminal Justice Data. Web site: *http://www.icpsr.umich.edu/ NACJD/welcome.html.*

National Research Council. *A Question of Balance: Private Rights and the Public Interest in Scientific and Technical Databases.* Washington, DC: National Academy Press, 1999.

New York Area Data Council, "Making the Best Use of Government Data," white paper, New York City, July 1999.

Official California Legislative Information, Web site: *http://www.leginto.ca.gov.*

Olligschlaeger, Andreas, "What is the appropriate model for partnerships between law enforcement agencies and researchers with regard to data sharing?" CMRC, July, 1999. Retrieved February 2001 from the World Wide Web: *http://www.ojp.usdoj.gov/ cmrc/pubs/privacy/olligschlaeger.pdf.*

Rich, Thomas, Abt Associates, phone interview on June 13, 2000.

Rich, Tom, "Crime Mapping by Community Organizations: Initial Successes in Hartford's Blue Hills Neighborhood," in *Crime Mapping Case Studies: Successes in the Field*, ed. Nancy La Vigne and Julie Wartell, Washington, DC: Police Executive Research Forum, 1998.

Schemo, Diana Jean, "Colleges Rushing to Compile Crime Statistics for the Web." *New York Times,* October 19, 2000. Retrieved October 22, 2000, from the World Wide Web: *http://www.nytimes.com.*

Statistical Efficiency Act of 1999, 106th Congress, 1st session, H.R. 2885.

U.S. Census Bureau. Web site: *http://factfinder.census.gov/html/ confidential.html.*

U.S. Office of Management and Budget. Web site: *http://www.whitehouse.gov/ OMB/memoranda/m99-18.html.*

Wilson, Larry, *Rookie's Guide to Creating WebSites*, Self-published, 1998. Retrieved February 2001 from the World Wide Web: *http://www.copseek.com/beatpress.*

Appendix A: Local Law Enforcement Disclaimers

Oakland (California) CrimeWatch

http://www.oaklandnet.com/maproom/cwdisclaimer.cfm

The crime icons are intended to indicate the block in which the crime allegedly occurred. The crime icons do not reflect the exact location of any particular crime.

The City of Oakland intends that the information provided by this Web site is accurate; however, errors sometimes occur. There are no implied or express warranties on the materials in this site; the materials that are provided will be subject to revision. Use this service at your own risk.

This service does not reflect official crime index totals as reported to the FBI's Uniform Crime Reporting program. The listed crimes are subject to change for a variety of reasons, including late reporting, reclassification of some offenses, and discovery that some offenses were unfounded.

In using this site the user understands and agrees with the above.

San Diego County ARJIS

http://www.arjis.org/mapping/help/disclaimer.html

This Web page is a public resource of general information. The Automated Regional Justice Information System (ARJIS) does not make any warranty, representation or guaranty as to the content, sequence, accuracy, timeliness, or completeness of any of the database information provided herein for any reason. All aspects of the data provided herein are susceptible to a degree of error due to the complexities of the process involved in compiling and programming the data.

All materials contained on this site are distributed and transmitted "AS IS" without warranties of any kind, either express or implied, including, without limitation, warranties of title or implied warranties of merchantability or fitness for a particular purpose. In no event shall ARJIS nor its member agencies become liable to users of these data for any loss or damages, consequential or otherwise, including but not limited to time, money, or goodwill, arising from the use, operation, or modification of the data. The visual presentation of data is being provided strictly as a courtesy, and not as an obligation to its readers. ARJIS and its member agencies do not have the available staff to assist in the interpretation of the data presented herein.

The ARJIS Web site should not be relied upon for emergency services and is in no way designed to serve as an alternative to emergency services provided by the 911 emergency telephone service. If you have an emergency or important time-sensitive crime information, please communicate this information to the appropriate law enforcement agency within your jurisdiction through the 911 emergency telephone service.

Salt Lake County Sheriff

http://www.slsheriff.org/sh/html/stats/disclaimer.html

The maps displayed on this Web site are susceptible to a degree of error due to the collection, entry, and geoprocessing of the data. No warranty or guarantee is made nor implied regarding the content, geographic

accuracy, timeliness, or completeness of the data. The maps are provided strictly as a courtesy to the public. The Salt Lake County Sheriff's Office does not have staff available to assist in the interpretation of the map content.

Sacramento Police Department

http://citymaps.sacto.org

This Web page is a public resource of general information. The city of Sacramento makes no warranty, representation, or guaranty as to the content, sequence, accuracy, timeliness, or completeness of any of the database information provided herein. The reader should not rely on the data provided herein for any reason. The city of Sacramento explicitly disclaims any representations and warranties, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose. The city of Sacramento shall assume no liability for:

1. Any errors, omissions, or inaccuracies in the information provided regardless of how caused; or

2. Any decision made or action taken or not taken by reader in reliance upon any information or data furnished hereunder.

http://citymaps.sacto.org/GISAPPS2/ cdisclaimer.htm

There are some important things that you need to know about before using this data!

1. All aspects of the data provided herein are susceptible to a degree of error due to the complexities of the process involved in compiling and programming the data. No warranty, representation, or guaranty is made or implied regarding the content, sequence, accuracy, timeliness, or completeness of the data provided herein.

2. This visual presentation of data is being provided strictly as a courtesy, and not as an obligation, to its readers. The police department does not have staff available to assist in the interpretation of the data presented herein.

Note: Crime data will not be displayed if you zoom in beyond a certain level of detail. All other layers will continue to be displayed in the map area.

Appendix B: Security Issues and Resources*

The following information is provided to give a broad background of the security issues related to data and map sharing with other agencies and the public. Many of the terms and explanations are technical and should be explored in greater depth or referred to security specialists if your agency is interested in pursuing that angle.

First, an agency needs to ask itself the following questions when facing data security issues:

1. What is being protected?

2. From whom is it being protected?

3. Do we have the internal staffing expertise to handle security issues?

4. For whom is the data intended?

5. How much time will have to be spent maintaining the system's security infrastructure?

6. Do our vendors place a high priority on security issues? Are they open about problems, and do they provide quick support for fixes to new problems?

There are several considerations for managing data security issues. Strategies to manage security for these considerations will vary depending on the network environment—LAN/WAN, Intranet, Internet, or Extranet.

Data. There are multiple ways of handling data security, including field suppression, substitution of records, aggregation (e.g., into blockgroups or ZIP Codes), generalization (e.g., to 100 blocks), sampling, and continuous surfaces instead of points.

Access control and authentication. Access can be restricted through password protection, leased lines, dial-up connections, and firewalls.

Encryption. Secure transmission can be accomplished with secure sockets layer, virtual private networks (VPN), public key infrastructure (PKI), and pretty good privacy (PGP).

Intrusion detection and weakness testing. To detect intruders and identify security weaknesses, the agency must be constantly vigilant and have well-trained personnel and a commitment on the part of management to provide resources for the most secure environment possible.

Organizational approach. Certain security issues can be overcome by using outside parties. This might include a regional crime mapping center as an expert-staffed clearinghouse and single point of defense and entry, a university partner as the security brain trust, or outsourcing to a third-party provider.

Agencies—large and small, technologically beginning or advanced—have faced similar problems. Some of the most common problems associated with data security are the following:

■ Sites do not install vendor patches for known problems.

■ Sites do not implement or enforce procedures and standards when adding new nodes or hosts.

■ Sites do not monitor or restrict access to host computers.

- Sites do not screen personnel with access to hosts.

- Sites do not use the best available authentication procedures.

- Sites do not dedicate sufficient resources or planning to security.

- There is insufficient management support for network administration personnel.

- Vendors are not open about security problems or prompt about fixing known deficiencies.

The following are some suggestions related to addressing security issues:

- Legitimize digital signatures as legally binding.

- Be aware of the widespread availability of strong encryption.

- Encourage Internet-based commerce.

- Make security primary when transferring any sensitive data.

- Consider security issues whenever a new infrastructure is put in place.

- Cultivate personnel with expertise in security issues.

- Consider a regional center as the data transfer clearinghouse.

- Create guidelines for public access to visualizations of crime data.

- Demand more openness on the part of vendors concerning security weaknesses in their products.

Security Resources

Although constantly changing and not to be construed as an endorsement of any company or products, the following list of resources may be used to obtain more information on security issues.

Web sites

SecurityFocus: *http://www.securityfocus.com.* Online security portal; clearinghouse on security information, including a vulnerability database and detailed articles on how to secure particular operating systems.

SecurityWatch: *http://www.security watch.com.* Online security portal; latest information on business, technology issues, bugs and fixes, and product updates.

SecurityPortal: *http://www.securityportal. com.* Online security portal; resource and service provider for companies and individuals concerned about protecting their information systems and networks.

CERIAS: *http://www. cerias.purdue.edu/.* University center for multidisciplinary research and education in areas of information security (computer, network, and communications security), and information assurance.

System Administration, Networking and Security Institute: *http://www.sans.org.* Resource for system and security alerts and news updates, special research projects and publications, education, and certification.

Internet Security Systems (ISS) Library: *http://xforce.iss.net/.* Resource database for computer threats and vulnerability.

Microsoft: *http://www.microsoft.com/ security/default.asp.* Headlines, bulletins, tools, and best practices.

Microsoft Internet Information Server (IIS) Security Checklist: *http://www. microsoft.com/technet/secrity/iischk.asp.* Steps an agency should take to secure a server.

RSA Laboratories FAQ: *http://www. rsasecurity.com/rsalabs/faq/index.html.* Frequently asked questions about cryptography.

VPN Source Page: *http://www.intenetwk. com/VPN.* Information and resources for virtual private networks.

NT Bugtraq: *http://www.ntbugtraq.com.* Mailing list for the discussion of security exploits and security bugs in Windows NT and its related applications.

Books

Hughes, Larry J., Jr. *Actually Useful Internet Security Techniques*, Indianapolis, IN: New Riders Publishing, 1995.

Chapman, Brent, and Elizabeth Zwicky. *Building Internet Firewalls*, Cambridge, MA: O'Reilly & Associates, Inc., 1995.

Ford, Warwick. *Computer Communications Security: Principles, Standards Protocols and Techniques,* Upper Saddle River, NJ: Prentice Hall, 1994.

Bernstein, Terry, Anish B. Bhimani, Eugene Schultz, and Carol A. Siegel. *Internet Security for Business*, New York, NY: John Wiley & Sons, 1996.

Garfinkel, Simson. *PGP: Pretty Good Privacy*, Cambridge, MA: O'Reilly & Associates, Inc., 1994

Rubin, Aviel D., Daniel Geer, and Marcus J. Ranum. *Web Security Sourcebook,* New York, NY: John Wiley & Sons, 1997.

Software

docSpace: *http://www.docspace.com.* File sharing on the Web; creates single URL for sharing large data files; secure Web courier service and Web-based collaboration; PKI used for authentication.

Tripwire for Windows NT: *http://www. tripwiresecurity.com.* Looks for traces of tampering by scanning for changes in system files and the registry; last line of defense.

ISS Inc: *http://www.iss.net.* Internet Scanner (vulnerability probe to check hosts from outside) and System Scanner (to check the host itself).

PGP Distribution Site at MIT: *http://web. mit.edu/network/pgp.html.* Software products for security, privacy, and strong authentication.

Computer Incident Response Teams

CERT Coordination Center at Carnegie Mellon University: *http://www.cert.org.* Study Internet security vulnerabilities and provide technical assistance.

Computer Incident Advisory Capability (CIAC) at U.S. Department of Energy: *http://www.ciac.org/ciac.* Bulletins, virus database, and other security tools.

Federal Computer Incident Response Capability (FIRST): *http://www.first.org.* Maintains incident response team lists.

---

* This information was taken from a presentation given by Robert Cheetham, Senior GIS Developer, Mayor's Office of Information Services, Philadelphia, Pennsylvania, at the CMRC Roundtable in 1999. The authors provided full citations for the book references.

Appendix C: Glossary

Aggregate data. Data describing the characteristic(s) of an area rather than an individual point. Often, individual point-level data are summed to an area boundary to use census or other grouped information. For example, individual incidents of burglary that occur within a census block or tract are often summed to provide a total number that occur in each area. This allows other census data to be used in conjunction with crime data to compare rates or develop models.

Choropleth map. A map depicting area boundaries in which the areas are shaded by the number or rate of a data variable present. An example would be a map of a city in which beats are shaded light green to dark green based on the number of property crimes or on the average household income.

Encryption. Process of encoding data to make them unreadable to those who do not have the key for deciphering them. Encryption is the technology of choice for protecting data in storage and during transmission over an insecure channel.

Geocoded data. Data that have been assigned locations on the earth's surface. Geocoding is the process of converting tabular data into a GIS format. For further explanation, see "Issues and Guidelines" in chapter 2.

Hit rate. Percent of incidents successfully geocoded (assigned an x,y coordinate). For example, if there were 10,000 auto thefts and the geocode rate was 90 percent, then 9,000 of those incidents would be available for mapping and analysis.

Hot spot map. A map depicting the areas of a beat, district, or city that have the densest concentration of a crime or incident. One type of hot spot map draws ellipses to delineate areas of high concentration. Another type computes a density across a geocoded area and shades each grid cell with the density value—the darker the shading, the denser the value.

Isopleth map. A map that is shaded without regard to boundaries. A weather map or shaded hot spot map (see definition above) are common examples.

Metadata. Information about the data. The Federal Geographic Data Committee requires 58 minimum fields, including identification information, such as originator, dates, purpose, coordinates, keywords, and graphic names; spatial data organization information; distribution information, such as contact person and contact information, resource description, and distribution liability; and metadata reference information, such as date, contact person, and contact information. Quality metadata is essential to successful data sharing.

Scale. The ratio between the distance on the map and corresponding distances in the real world. With a small scale, features appear small and show a small amount of detail (e.g., a globe). With a large scale, features show large and show large amounts of detail (e.g., parcel maps).

Spatial data. Data that have been assigned locations in geographic space and can be depicted on a map.

Appendix D: MOU Examples

MEMORANDUM OF UNDERSTANDING FOR THE BALTIMORE REGIONAL CRIME ANALYSIS SYSTEM COORDINATING COMMITTEE

REGIONAL CRIME ANALYSIS SYSTEM

The member agencies of the Regional Crime Analysis System (hereinafter referred to as "RCAS") enter into this Memorandum of Understanding in order to set forth agreements and protocols that will guide their interaction with, contributions to, and handling of information from the computerized database/programs which are the cornerstone of the system.

I. INTRODUCTION AND BACKGROUND

Law enforcement agencies have known and understood for decades that criminal activity does not recognize jurisdictional boundaries. Criminals are aided by their freedom from these jurisdictional boundaries as much as they are by their unfettered access to private transportation and regional transportation systems; they can and do take advantage of the restrictive jurisdictional boundaries by which law enforcement agencies are bound, abetted by the law enforcement community's traditional lack of systematized inter-jurisdictional information sharing technologies and protocols.

In order to prevent and suppress crime, it is critical that law enforcement agencies develop methods of timely information sharing which can be used to link individual criminal acts and also identify those responsible for committing those acts.

To date, information sharing across jurisdictional boundaries has been accomplished by periodic word of mouth and/or written correspondence. Recent advances in communication and computer technology now enable jurisdictions to share timely information electronically. Sharing information in this fashion will speed criminal activity trend detection, resulting in more efficient and effective police operations.

II. THE ROLE OF THE REGIONAL CRIME ANALYSIS SYSTEM

It is the intent and purpose of the participating agencies (hereinafter referred to as "members") to establish and maintain a Regional Crime Analysis System (RCAS) to improve the ability of the region's various law enforcement agencies (members) to monitor and analyze criminal activity in, and in areas surrounding, their own jurisdictions; to improve each members' ability to recognize and respond to evolving crime patterns; to enhance regional operational planning; to improve regional decision-making; and to enhance the information each member has available upon which to base decisions concerning the allocation and deployment of resources for the prevention and suppression of criminal activity.

A. Members agree to establish a RCAS Oversight Committee, to be composed of one member from each member agency. The RCAS Oversight Committee shall:

- meet at least quarterly, to discuss problems, suggestions for improvements, purchase decisions, violations of this agreement, or new membership applications.

- have the authority to establish and modify the rules and regulations governing membership and the operation of the RCAS system.

- base all decisions and actions on a majority vote of member agencies.

■ select a RCAS Oversight Committee Chairperson on a rotating basis, as decided by the Committee. The Chairperson shall hold the position for one year.

■ select a RCAS Oversight Committee Vice-Chairperson who shall oversee the collection, handling, disposition and control of all fees collected.

B. Member agencies shall provide crime data to the RCAS system and ensure the security of RCAS in accordance with procedures established by the RCAS Oversight Committee.

C. Information developed through analysis of RCAS data is for the benefit of member agencies and shall not be released to others.

D. There shall be an annual non-refundable fee of one thousand dollars ($1,000.00) assessed to each member agency, to establish and maintain shared resources. Agency fees will be kept in an interest-bearing account established by the Oversight Committee, and all disbursements will require two signatures: that of the Oversight Committee Chairperson and Vice-Chairperson. Fees will be due no later than ninety (90) days after July first of each year. Non-payment of fees will be referred to the Oversight Committee for action.

E. Individual member agencies shall be responsible for all local costs associated with their agency's data provision, conversion and analysis, and all local communication equipment and software required to connect their agency to the system.

F. Member agencies can terminate their participation at any time by written notice to the Oversight Committee.

G. In the event of the dissolution of the RCAS, any remaining funds will be divided among all member agencies in good standing. The division of funds will be determined by the RCAS Oversight Committee.

III. LIABILITY FOR PARTICIPATION IN THE REGIONAL CRIME ANALYSIS SYSTEM

Since participation in RCAS is voluntary, member agencies:

■ acknowledge that the activities and provision of services hereunder are subject to the budgetary, purchasing procedures, and available resources of each agency;

■ shall remain liable for the acts and omissions of their employees; and,

■ are self-insured or agree to maintain adequate comprehensive general liability insurance, to meet the obligations of this memorandum of understanding.

BY OUR SIGNATURES we hereby agree to the terms herein set forth.

For Anne Arundel County   **For Howard County**

_____   _____
Signature   Date   Signature   Date

For Montgomery County   **For Maryland State Police**

_____   _____
Signature   Date   Signature   Date

For Baltimore County   **For Prince George's County**

_____   _____
Signature   Date   Signature   Date

MEMORANDUM OF UNDERSTANDING FOR THE MEMPHIS AREA "COMMUNITY SAFETY INFORMATION SYSTEM"

This agreement is entered into between the City of Memphis Police Department, hereinafter referred to as "MPD," and the undersigned User Agencies, hereinafter referred to as "Agency," on the _____day of _____, 20___. This agreement shall set forth the guidelines for the sharing of data and mapping technologies through a centrally located server via the Internet, which shall be maintained by the Memphis Police Department within the terms, conditions and stipulations herein described. An Agency may withdraw from this agreement by providing 90 days of advanced notification, in writing, to the Director of Police Services, City of Memphis Police Department.

WHEREAS, the Community Safety Information System, hereinafter referred to as CSIS, was initiated by the National Institute of Justice in order to increase the capacity of the US Attorneys to work in partnership with federal, state, and local criminal justice agencies and research entities.

AND WHEREAS, the CSIS is highly desired by User Agencies, who are interested in forming a partnership in order to collaborate on data collection and analysis, to design targeted strategies, to plan interventions that will prevent crime and increase community safety, and to enhance the working partnership of the Agencies involved in this agreement.

NOW THEREFORE, in consideration of the terms and conditions contained within this agreement, the undersigned agencies agree as follows:

1. An "Agency" shall be defined as any agency having signed this agreement to have access to the CSIS system;

2. A "Data Contributing Agency" shall be defined as any agency having signed this agreement to have access to the CSIS system and one which provides data in support of the systems operation;

3. The following are Data Contributing Agencies:

   Memphis Police Department
   Shelby County Sheriff's Office
   Memphis and Shelby County Juvenile Court
   Tennessee Board of Probation and Parole
   Memphis Sexual Assault Resource Center

4. The following are Agencies that shall have access to the CSIS system:

   Memphis Police Department
   Shelby County Sheriff's Office
   U.S. Attorney's Office
   Memphis and Shelby County Juvenile Court
   Tennessee Board of Probation and Parole
   Shelby County Attorney General's Office
   Memphis Sexual Assault Resource Center
   Child Advocacy Center
   Victim's Assistance Center
   Shelby County Department of Corrections
   Shelby County Pre-Trial Services
   Memphis Shelby Crime Commission
   University of Memphis
   University of Tennessee

5. Each Data Contributing Agency shall appoint one member from their agency to the "Systems Governance Committee". This member shall represent their respective agency interests as related to technology issues, liability, data information/security, data standards, operations, planning, development of new services, upgrades, integration and other related issues to the operation of the system. The University of Memphis shall have one ex officio member on this committee. The Systems Governance Committee shall meet quarterly or on a more often basis if the committee determines a need exists. The chair of the Systems Governance Committee shall be elected by a majority vote of the committee members and serve for a period of one year;

6. All Agencies accessing the system shall be bound by local, state and federal laws applicable to the operation of the system known as CSIS;

7. All Agencies shall be further bound by the rules, regulations, guidelines, user agreements, etc. determined by the "Systems Governance Committee" for CSIS;

8. All Data Contributing Agencies, their governments, agents and representatives, assume no liability and shall be held harmless from any legal actions arising from the use of CSIS system by other Agencies who share access to the system. The "hold harmless" requirement of this provision shall not be applicable to the University of Memphis. Any and all claims against the State of Tennessee, including the University, its employees, agents, or representatives, arising out of this Memorandum of Understanding shall be submitted to the Board of Claims or Claims Commission of the State of Tennessee. Damages recoverable against the University shall be expressly limited to claims paid by the Board of Claims or Claims Commission pursuant to Tenn. Code Ann. Section 9-8-301, et. seq;

9. MPD shall maintain the computer server to house all records capable of entry into the system and any applicable interfaces, and shall maintain a back-up system to retrieve data in the event of catastrophic failure, but makes no guarantee that all back-up records will be available;

10. All Agencies shall connect to the CSIS system via the Internet.

11. Each Agency accessing the system shall be responsible for their own cost of connectivity to CSIS via an ISP, Internet Service Provider;

12. Each Agency shall be responsible for the cost of training, software licenses and any maintenance agreements necessary for the use of the system within their agency;

13. Each Agency shall be individually responsible for the repair, service, maintenance, upkeep, etc. of PC's, servers, peripherals, fiber, data lines, software applications, modems, communication devices, switches, routers, etc., which are not owned or operated by the MPD in support of CSIS;

14. The CSIS System shall be limited to 10 concurrent users to prevent system degradation and MPD reserves the right to maintain the security necessary to protect the system from intruders and unauthorized use of CSIS and the MPD Network;

15. Data Contributing Agencies shall be required to maintain up-to-date industry standard virus protection on all computer equipment used to download data for entry into the system;

16. Data Contributing Agencies shall provide data for entry into the CSIS in a timely manner as determined by the Systems Governance Committee;

17. Data Contributing Agencies failing to provide data for the CSIS in a timely manner, as determined by the Systems Governance Committee, shall have access rights terminated upon a majority approval of the Systems Governance Committee;

18. MPD shall be responsible for the systems administration of CSIS, to include users' rights for access, adding of records and data that are to be available in the CSIS system, as provided by Data Contributing Agencies in consultation with NIJ and the Indus Corporation and their representatives;

19. All Agencies shall ensure the integrity of CSIS is maintained by ensuring User Names and Passwords are not shared and meet current and acceptable industry standards as defined by the Systems Governance Committee. A breach in security shall be seen as serious and will be handled accordingly;

20. Data Contributing Agencies shall require that data entry standards, necessary for the operation of the CSIS, are met to ensure the accuracy of data put in the system;

21. Access to all data shall be restricted to "read and print only" and is restricted to user authorization, as determined by the Agency sharing the system to ensure the integrity of the system, and to protect any confidential data from unauthorized access or viewing and as required by local, state and federal laws and as described in this agreement;

22. Data entered into the CSIS is solely owned by the Data Contributing Agency who provided the data;

23. Data Contributing Agencies reserve the right to determine what data will be provided for entry into the CSIS system and such data must be applicable to the operation of the system;

24. No Agency shall through this agreement or any other agreement sell, distribute, issue, circulate, allow access, etc., to data provided by any Data Contributing Agency or access to the CSIS system, except as provided and authorized in this agreement;

25. MPD shall operate the system, as long as it is reasonably cost effective to do so and the system meets current technological and information needs of the Agencies involved. In no event shall MPD terminate this agreement and discontinue use of CSIS without providing 12 months of advanced notification to any Agency using the system;

26. All other terms and conditions, not described herein, are exclusively maintained by MPD.

WITNESS the signatures of the respective parties by their authorized officers on the day and year written above.

MEMPHIS POLICE DEPARTMENT

_____

U.S. ATTORNEY'S OFFICE

_____

TENNESSEE BOARD OF PROBATION AND PAROLE

_____

CHILD ADVOCACY CENTER

_____

SHELBY COUNTY DEPARTMENT OF CORRECTIONS

_____

MEMPHIS SHELBY CRIME COMMISSION

_____

SHELBY COUNTY ATTORNEY GENERAL'S OFFICE

_____

SHELBY COUNTY SHERIFF'S OFFICE

_____

MEMPHIS AND SHELBY COUNTY JUVENILE COURT

_____

MEMPHIS SEXUAL ASSAULT RESOURCE CENTER

_____

VICTIM'S ASSISTANCE CENTER

_____

SHELBY COUNTY PRE-TRIAL SERVICES

_____

UNIVERSITY OF MEMPHIS

_____

UNIVERSITY OF TENNESSEE

_____

Revised 8–1–2000

About the National Institute of Justice

NIJ is the research and development agency of the U.S. Department of Justice and is the only Federal agency solely dedicated to researching crime control and justice issues. NIJ provides objective, independent, nonpartisan, evidence-based knowledge and tools to meet the challenges of crime and justice, particularly at the State and local levels. NIJ's principal authorities are derived from the Omnibus Crime Control and Safe Streets Act of 1968, as amended (42 U.S.C. §§ 3721–3722).

NIJ's Mission

In partnership with others, NIJ's mission is to prevent and reduce crime, improve law enforcement and the administration of justice, and promote public safety. By applying the disciplines of the social and physical sciences, NIJ—

• **Researches** the nature and impact of crime and delinquency.

• **Develops** applied technologies, standards, and tools for criminal justice practitioners.

• **Evaluates** existing programs and responses to crime.

• **Tests** innovative concepts and program models in the field.

• **Assists** policymakers, program partners, and justice agencies.

• **Disseminates** knowledge to many audiences.

NIJ's Strategic Direction and Program Areas

NIJ is committed to five challenges as part of its strategic plan: 1) **rethinking justice** and the processes that create just communities; 2) **understanding the nexus** between social conditions and crime; 3) **breaking the cycle** of crime by testing research-based interventions; 4) **creating the tools** and technologies that meet the needs of practitioners; and 5) **expanding horizons** through interdisciplinary and international perspectives. In addressing these strategic challenges, the Institute is involved in the following program areas: crime control and prevention, drugs and crime, justice systems and offender behavior, violence and victimization, communications and information technologies, critical incident response, investigative and forensic sciences (including DNA), less-than-lethal technologies, officer protection, education and training technologies, testing and standards, technology assistance to law enforcement and corrections agencies, field testing of promising programs, and international crime control. NIJ communicates its findings through conferences and print and electronic media.

NIJ's Structure

The NIJ Director is appointed by the President and confirmed by the Senate. The NIJ Director establishes the Institute's objectives, guided by the priorities of the Office of Justice Programs, the U.S. Department of Justice, and the needs of the field. NIJ actively solicits the views of criminal justice and other professionals and researchers to inform its search for the knowledge and tools to guide policy and practice.

NIJ has three operating units. The Office of Research and Evaluation manages social science research and evaluation and crime mapping research. The Office of Science and Technology manages technology research and development, standards development, and technology assistance to State and local law enforcement and corrections agencies. The Office of Development and Communications manages field tests of model programs, international research, and knowledge dissemination programs. NIJ is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

To find out more about the National Institute of Justice, please contact:

National Criminal Justice Reference Service
P.O. Box 6000
Rockville, MD 20849–6000
800–851–3420
e-mail: *askncjrs@ncjrs.org*

To obtain an electronic version of this document, access the NIJ Web site
(*http://www.ojp.usdoj.gov/nij*).

If you have questions, call or e-mail NCJRS.