Computer Mapping and Data Protection

A joint publication by NIJ's
Crime Mapping Research Center and
the Institute for Law and Justice

July, 2000

Chapter I Outline

I. The Problem of Mapping and Data Confidentiality

A. Several trends have resulted in greater availability and access of information to the public.

1. Several technological advances have occurred in computers and GIS applications.
2. Computer hardware is smaller and cheaper, yet more powerful.
3. Telecommunications to connect users to computers is easier.
4. Use of the Internet is increasing.
5. Service providers, such as AOL, have emerged for easier connectivity.
6. Diverse data sets can be merged more easily than in the past.
7. Software for desktop and Internet mapping has made great strides.
8. Statistical tools for analyzing spatial data are improving steadily.

B. Citizens have a desire for access to data.

1. Many citizens take interest in their communities.
2. Crime-related information is always a popular subject.

3. Police and citizens are working together in many communities to solve local problems, with mapping as one tool.

C. Police departments continue to have interest in information technologies.

1. Police operations are information driven.
2. Police officers and their leadership are more comfortable with technology and its use for analysis and decision making.
3. Police would like to use technology, such as the Internet, to reduce requests yet still provide services to the community.

D. Several problems have emerged because of these developments.

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 these rights be balanced?
2. Other interested persons, especially researchers, want access to geocoded data on crime. How can these data be provided without violating victims' rights?
3. If geocoded data are made available to others, what are the liability issues on misuse of the data?
4. If police departments make crime data available on the Internet, what security measures need to be taken to minimize risk of intrusion?

E. The purpose of this report is to provide guidance on these issues.

1. Several topics are covered:
   a. Benefits of providing maps to citizens, other agencies, and researchers.
   b. Privacy issues and how to address them.
   c. Development of local guidelines for desktop and Internet mapping.
   d. Examples of agencies that have successfully done mapping.
   e. The need for disclaimers when providing maps and data on the Internet.

f. Geocoding “hit rates” and the need to disclose these rates when providing maps.

g. Issues surrounding the availability of maps on the Internet.

2. The target audiences for this publication are police managers responsible for making decisions about what will be mapped, personnel responsible for mapping, researchers, and web site developers.

3. Contents of report are based on:

   a. Papers prepared by several researchers and practitioners across the country.

   b. The *Crime Mapping and Data Confidentiality Roundtable* held in July 1999.

   c. A review of how other federal agencies have approached similar problems.

   d. Discussions at three mapping conferences sponsored by the NIJ Crime Mapping Research Center.