



**Crime Mapping and  
Data Confidentiality Roundtable  
July 8-9, 1999  
Sponsored by: National Institute of Justice,  
Crime Mapping Research Center**

**Where is the Balance Between the Public's Right to Know  
and the Victim's Right to Privacy?**

**by  
Chief Jim Bueermann,  
Redlands (CA) Police Department**

**Statement of the Issue**

The societal use of GIS has expanded at a phenomenal rate over the last twenty years. In the early 1980's there were several hundred people using GIS today there are over 250,000 with the number growing daily. Only in the last few years have the police and other components of the criminal justice system really discovered the power this technology affords. Daily, police websites are created that afford the public unprecedented access to sophisticated GIS databases of crime incidents in a variety of formats everything from density maps to address level data. So far, advances in computer/GIS technology have outpaced the evolution of public policy relative to the use of GIS data. A pivotal policy question to be addressed regarding the use of this data is: *where is the balance between the public's right to know and the victim's right to privacy?*

**Trends Affecting the Issue**

Trends which are having an impact on this issue include:

- technological advances in computers and GIS applications
- power/capacity/user-friendliness/internet mapping;
- societal awareness of the power of GIS
- citizen demands for access to data which form the basis for public decision making;
- the continual evolution of community-oriented policing practices which place an emphasis on citizen collaboration and data-driven decision making;
- an increasing awareness of the inter-connectedness of data and processes within and outside the criminal justice system;
- police leadership becoming more comfortable with, and drawn to, technological advances in the area of organizational analysis and decision making; and,
- the increase in police entrepreneurialism in which police organizations develop revenue streams out of their activities (i.e. software development,

dispatching/computer out-sourcing, etc.) that may result in an appreciation of the value to the private sector (e.g. security companies, realtors) of geocoded police data.

### **The Public's Right to Know**

One of the most fundamental underpinnings of our democratic society is the recognition that the public has an inherent right to know, in most cases, about the activities of its governmental organizations. This is especially true about the majority of the activities reported to, or initiated by, the police. The police blotter has long been the traditional forum for informing the public about police activities. The nature of police actions, their outcomes, their dates and times, adult arrestees' names, and importantly, *their locations* have been the essence of such reporting. With the advent of GIS technology the publication of crime maps is becoming commonplace. This type of data is acquired, analyzed and relied upon to form the basis of many public policies all at taxpayer expense.

There is a compelling public interest in knowing where crime is located. People want to know, and have a right to know, the nature of crime in their communities and *where* it is occurring. It has long been established police practice, and in most states it is a statutory requirement, to release the basic facts of most criminal incidents. Therefore, the public already has a familiarity with the disclosure of crime data which will likely evolve into an appetite for crime maps to easily display the nature of crime in our communities.

### **Protecting a Victim's Right to Privacy**

The exception to crime data disclosure practices and rules is usually found in cases relating to sexual assaults and/or those cases involving juveniles. The notion that public disclosure of a sexual assault victim's name, address, etc. will further victimize her/him has long been accepted by the criminal justice community, the media and the public. The pivotal question in protecting a victim's right to privacy is: *how can crime data be displayed without compromising the identity of the victim?*

While it is clear that releasing the victim's name, address, etc. will violate this intent, can less obvious practices do the same? Mapping address level incidents, or allowing access to crime mapping databases can serve to violate victim confidentiality as effectively as the release of their name and address.

### **Possible Solutions**

The following are a few practices that can be employed to maintain victim confidentiality while also providing the public with a reasonable amount of information regarding crime:

- using symbols large enough to obscure address level mapping;
- removing streets from maps at a level sufficient to hide address-level awareness of where a crime occurred;
- releasing thematic maps as opposed to address-level maps; and,
- restricting crime database access to the public.

### **Policy Implications/Recommendations**

It seems clear that there is a compelling need for public policy regarding the use and release of geocoded crime data. The creation of a national model policy would provide criminal justice agencies a standard with which they could use in formulating their own specific policy. This is a much preferred alternative to a judicial or legislative mandate formulated as a result of a well-intended, but unfortunate release of restricted information.