Evidence Generated from GIS

Harlan J. Onsrud
Department of Spatial Information Science and Engineering
University of Maine

INTRODUCTION

In modern cartographic and surveying practice, maps and survey plats traditionally maintained as paper documents are now being maintained in digital form in computerized files. In addition to data inaccuracy and data imprecision, potential errors associated with geographic information systems and other computerized spatial handling systems include input, hardware, software, modeling and perception errors. Because of these potential errors and because digital data is relatively easy to alter with little or no trace, the legal reliability and stability of data from computerized land information systems have become important issues for users and potential users of such systems.

For purposes of evaluating the admissibility of GIS evidence in court, let us assume four separate scenarios:

**Scenario 1:** An environmental conservation group has used a GIS to track the existence and location of plant and animal species over an extended period of time on a large parcel of land it owns. The group claims that adverse effects caused by the presence of a recently built nearby shopping center are destroying the ecosystem of their parcel. They claim the biodiversity of their parcel has been decimated and several species have been wiped out altogether. The group wishes to use their GIS evidence in a law suit for damages and to halt current plans for expanding the shopping center.

**Scenario 2:** An architectural firm purchased from a municipality a GIS data set that identified the locations and sizes of various buried utilities in the community. The architectural firm claims that some of the digital data provided to it was wrong, that the firm suffered major construction delay and redesign expenses due to the wrong data, a duty of reliability on the part of the city existed in providing the data, and that the city is liable for the damages suffered. (For a discussion of negligent dissemination by government of faulty data, see Dansby 1992). The city claims that the data it delivered to the architectural firm was essentially correct. Six months later during the discovery process in preparation for trial, it is determined that the architect's archived copy of the utility data set does not match the city's archived copy of the same data set, although the two files purportedly should be identical. The city claims that the digital files must have been altered by the architect or one of her employees, inadvertently or otherwise. The architect, however, claims that the city or one of its employees has altered its archived file in order to "cover its tracks" by correcting the faulty data prior to discovery. Just as a forged deed or contract should not be admitted for consideration at trial, the architect seeks
to have the city's "forged" digital data set held inadmissible. The city seeks a similar ruling on the architects archived file.

Scenario 3: A geographic information system has been used by city administrators to aid in various decision making processes. For instance, the GIS has been used as an aid in making decisions regarding tax assessments, zoning and districting delineations, permitting, distribution of social program services throughout the community, when and where to schedule maintenance of aging infrastructures, siting of new utilities, routing of school buses and emergency vehicles (police, fire, ambulance), and numerous similar decisions. A group of minority citizens claims that they have been adversely affected by numerous of the decisions reached through use of the city's GIS analysis capabilities. Rather than using the power of GIS and associated technologies to arrive at less emotional and more rational, neutral and logical decision making, the citizens group claims that the seductiveness of computerized data analysis and modeling has been used by city administrators to systematically favor certain groups in the community and discriminate against others. The citizens group claims city administrators have purposefully chosen search and buffer radii in use of the GIS in order to establish biased pools of comparable properties for tax assessment and zoning purposes, they have selected data generalization and aggregation techniques in order to purposefully arrive at configurations of data which support the results desired by the administrators, and they have carried out computerized gerrymandering in the drawing of various district lines. In other instances the citizens group claims that the data in the GIS was wholly inappropriate for the decisions made based on it, significant blunders exist in the data to the extent that rational decision making is not possible using the data, and there has been a lack of security in allowing access and alterations to data sets. City administrators claim that the charges are ridiculous and it is the citizens group that is stretching the bounds of reasonable data analysis, not the city. A discrimination lawsuit for several million dollars has been filed and both sides want their data analysis and modeling results admitted to prove the truth of the claims they are asserting.

Scenario 4: Litigation has commenced between an oil company and an adjoining landowner over the cause and extent of oil spill damage from a broken oil pipe. The oil company has used its in-house GIS capabilities incorporating pre-spill orthophotography overlain with post-spill imagery from a digital camera to map the physical situation on the ground immediately after the spill. The adjoining landowner argues that the digital imagery has been altered, that the extent of the alterations is impossible to discern, and that the imagery is so unreliable that it should not be admitted into evidence.

Each of the four scenarios raises varying questions regarding the principles that will be used by courts in allowing GIS evidence to be considered by the trier of fact in courtroom settings.

If the data contained within or the products generated from a specific operational GIS eventually are shown to be readily and successfully challengeable in court, much of the investment in the system may be lost. Decisions based on data from the system generally will no longer be considered reliable by the public. Therefore, land information system developers and managers should be aware of the general requirements for admissibility of computer generated evidence in court as well as be prepared to convince a panel of jurors of the reliability of the system.
Private firms and utilities which use automated mapping or geographic data processing systems to aid the productivity and decision making of their firms need to be just as aware of admissibility and reliability concerns. Increased liability exposure and the need to admit computer generated products into evidence to defend against possible tort actions (e.g. negligence) and breach of contract claims may provide added reason for these firms to be aware of such issues.

Today, the vast majority of computer-generated documents reaching the courtroom do so under the business records exception to the hearsay rule. However, in regard to GIS data or analysis results, other potential and likely routes for admissibility might be through an exception for public records maintained by a public agency, through any other statutory exceptions which might apply, as demonstrative evidence to aid the trier of fact (i.e. jury) in understanding the testimony, or for the limited purpose of showing the basis of an expert's opinion.

ADMISSIBILITY OF EVIDENCE

Evidence is the material offered in court to persuade the trier of fact about the truth or falsity of a disputed fact. Today, all federal courts adhere to the rules for admissibility published in an administrative law volume titled the Federal Rules of Evidence. State court systems adhere to similar sets of published rules. The Federal Rules of Evidence will be used for illustrative purposes in this discussion because many state court systems have rules of admissibility very similar to the federal rules and a certain proportion of cases involving the admissibility of computerized GIS files would be heard in the federal courts.

It should be noted that after hearing and considering issues of admissibility on a particular piece of evidence, a trial court's decision on the issue seldom will be questioned by a higher court relative to the types of GIS scenarios outlined above. Higher courts will typically require proof of a "clear abuse of discretion" before attempting to second guess a lower court's decision on admissibility matters.

1. Relevancy of the Evidence

The question of admissibility of evidence arises when one party offers evidence into trial and the opposing party objects. The first criteria in overruling the objection is that the evidence must be relevant to a proposition in issue. If the evidence has "... any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence..." it is relevant and is admissible unless excluded by a specific rule (Fed. R. Evid. 401 & 402). This is a rather lenient requirement and typically won't be an obstacle to admissibility of GIS evidence.

2. Hearsay Rule

The most frequently attempted method of excluding computer-generated exhibits, even though the exhibits may be relevant to an issue in dispute, is through the "hearsay rule". Hearsay is an "... oral or written assertion... other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted" (Fed. R. Evid. 801 (a) and (c)). The hearsay rule states that hearsay is inadmissible unless the evidence qualifies under a hearsay evidence exception (Fed. R. Evid. 802).

Data files stored in a computer and printouts generated from those files are considered to be out of court statements and when offered in court for the truth of what they assert, they are
deemed to be hearsay (King and Stanley 1985, p. 401). Computer generated printouts, maps, images, and models are seldom offered for other than proving "the truth of the matter asserted." Unless an individual happened to have designed and manufactured the computer hardware, wrote the GIS software, and carried out the product generation or database manipulation procedures involved in the dispute, a computer generated product (i.e. the written assertion by the individual declaring its truth) involves out of court statements by others and thus will almost always be deemed hearsay. Therefore, such products must almost always qualify under one of the hearsay exceptions.

a. Business Records Exception

The hearsay exception most often applicable in successfully admitting computer generated printouts into evidence is known as the business records exception. Federal Rules of Evidence 803(6) states:

The following (is) not excluded by the hearsay rule, even though the declarant is available as a witness:

(6) Records of Regularly Conducted Activity. A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness...

A data compilation in any form is acceptable. Although computer printouts on paper made at the time the relevant electronic data was collected or processed might be more convincing to a judge or jury, the rule does not require this. If certain kinds of digital files are always archived in the course of doing business, it is sufficient that the digital data was recorded at or near the time in question. If the date of electronic recording of the specific data can be reliably established, the computer-generated printouts of that data on paper for presentation in court may be made at any time (United States v. Russo, 480 F.2d 1228, 1240 (6th Cir. 1973)).

To be relevant and admissible, computer files created in the regular course of business must necessarily be authentic. Authentication "...is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims" (Fed. R. Evid. 901(a)). An illustration of authentication evidence for computer records conforming with the requirements of this rule is "...evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." (Fed. R. Evid. 901(b) (10)). This illustration has generally been understood by the federal courts to require that the proponent of the evidence must authenticate a computer generated business record by showing (1) the input procedures used to supply information to the computer, (2) the tests that were used to assure the accuracy and reliability of both the computer operations and the information that was supplied to the computer, and (3) the fact that the computer record was generated and relied upon in the regular course of business " (Comment 1982, p.956, Henak and Henak 1989, p.12)

Thus, the trend by the courts has been to set additional foundational requirements which must be met before computer-stored business records are authenticated. The authenticating witness does not have to be one of the programmers involved in developing the software. However, the authenticating witness must be familiar with all phases of the field and office procedures which produced the product or result in contention and be able to explain
succinctly why it is that errors and mistakes are unlikely to have crept into the system. These errors include "...errors in perception (e.g. misreading or misinterpreting data fed into the system), errors in input, errors associated with inadequate hardware security, errors caused by hardware, and errors associated with computer software" (Snyder 1989, p.105). Because the data placed in GIS are often dependent on measuring and interpretation processes, errors in results due to data precision and data accuracy also need to be accounted for. Therefore, GIS managers should be prepared to provide testimony that errors from each of these sources are highly unlikely to be present or the effects of the errors are negligible for the computer generated evidence in the factual situation before the court. This may be problematic.

The authentication requirements outlined are rather stringent and place a substantial burden on anyone trying to admit computer records into evidence. As a result, "(s)ome courts have ignored suggestions calling for the creation of special foundational rules for authenticating computerized evidence. Instead, these courts require only a custodian of records to testify that the computerized records were kept in the regular course of business" (Snyder, p. 105). In such courts the custodian need only testify that computer-generated records are what they purport to be and need not attest that the records are accurate. The judgment on the degree of accuracy and reliability to be accorded to the evidence is left almost entirely to the trier of fact. Storm presents several arguments why "... computer generated records should carry a strong presumption of reliability which only an equally strong showing of a lack of trustworthiness should overcome" (Storm 1984, p.125). It may be argued however that this judicial approach runs directly counter to the presumptive burden established by Rule 803 (6) cited previously which negates the admissibility of evidence if "the source of information or the methods or circumstances of preparation indicate lack of trustworthiness."

To avoid the harsh authentication tests, other judges have moved even further by allowing the admission of computer-generated evidence under some circumstances through judicial notice (Snyder, p.109). This is likely to occur only with computer-generated printouts from off-the-shelf computer programs which have been widely used throughout business for an extended period of time. Judges have reasoned in such instances that if a software system wasn't reliable, it would not have lasted in the marketplace.

It would be unwise for GIS managers to assume that judges might support a presumption of reliability or take judicial notice of the reliability of complex commercial GIS software in their current states of evolving development. Likewise, judges would be unlikely to support a presumption of the reliability of GIS databases or of the results or products generated from them. Such databases seldom adhere to formalized and accepted standards and GIS databases contain a range of error sources not found, for instance, in accounting or product inventorying databases. In addition, GIS database managers typically do not utilize the controls, auditing, and security measures which could justify a presumption of reliability for other types of regularly kept computer records.

Lynch and Brenson stress that under the business records exception, "...neither the "business" nor the "regularly kept" requirements guarantee that the data or program will produce a reliable or accurate result." (Lynch and Brenson 1989, p. 927). They urge that a meaningful assessment of the reliability of any computerized system requires that databases, input procedures and processing program must all be tested separately for accuracy. These arguments appear to be particularly germane in evaluating the reliability of GIS and the products generated from them.

In some State courts, the harshness of the hearsay rule as applied to computerized records is sometimes overcome by State legislation. For instance, Iowa, Virginia and Florida
statutes explicitly state that computerized records are admissible without further proof so long as made in the ordinary course of business. By example, the Iowa Code provides that:

Any writing or record, whether in the form of an entry in a book, or otherwise, including electronic means and interpretations thereof, offered as memoranda or records of acts, conditions or events to prove the facts stated therein, shall be admissible as evidence if the judge finds that they were made in the regular course of doing business at or about the time of the act, condition or event recorded, and that the sources of information from which made and the method and circumstances of their preparation were such as to indicate trustworthiness, and if the judge finds that they are not excludable as evidence because of any rule of admissibility other than the hearsay rule. (emphasis added) (Lynch and Brenson 1989, p. 923)

In the first scenario presented at the beginning of this paper, the argument might be made that the conservation group is not carrying out a "business" and therefore can not qualify under the business records exception. This argument, however, is not conclusive since even personal business records have gained admittance under the exception in the past. Additionally, the conservation group may argue that its "business", albeit non-profit, is to keep track of and protect the environmental status of the lands it acquires. They may also argue that they had no reason to lie about or distort the data when it was recorded. The opposing party may argue that during and after the shopping center was built they had ample opportunity and incentive to distort the data. Therefore, the conservation group's arguments of trustworthiness are weak unless they can show that their records are regularly relied upon in financial or other business dealings and they would be substantially harmed if their records were not accurate.

In the second and third scenarios the GIS files maintained by the cities and the architectural firm were generated or used in the regular course of business and therefore have a substantial likelihood of being admitted under the business records exception. Relative to the second scenario, the argument may be made that the possibility of tampering should not preclude the admissibility of the evidence. "If tampering is suspected, evidence may be produced showing that the records are not what they purport to be. The probative value accorded the evidence can then be determined by the trier of fact" (Snyder 1989, p.106). Whether the evidence of tampering is so extensive as to make it necessary to exclude the evidence altogether would be largely then a determination for the trial judge.

In scenarios three and four, the bodies of GIS evidence developed by the group of minority citizens and that gathered by the oil company were both generated in preparation for trial. Therefore, this evidence is not likely to be admitted under the business records exception. These bodies of evidence, however, may reach the courtroom through other means.

b. Other Hearsay Exceptions

There are 23 specific exceptions to the federal hearsay rule as well as a general exception provision (Fed. R. Evid. 803). Of the specific hearsay exceptions, the one likely to find the next greatest utility in the admissibility of GIS evidence is the "public records and reports exception."

Numerous public agencies at the federal, state, and local levels are establishing automated land information systems for a variety of purposes. When a printout submitted for admission is a copy of electronic files collected and maintained by a public agency as a public record or document (i.e. "... a data compilation, in any form, of public offices or agencies, setting forth ... the activities of the office or agency, ....") and the printout is certified as a correct copy by a custodian of the records or some other authorized person,
the printout is self-authenticating and no extrinsic evidence of authenticity is necessary (Fed. R. Evid. 803).

Additionally, legislation in some States may name specific government computerized records that are explicitly exempted from the hearsay rule (e.g. Alabama Department of Revenue records - Ala. Code ss. 40-2-12 to 40-2-14 (1989), Florida Department of State required filings - Fla. Stat. s. 15.16 (1989), Georgia Crime Information Center records - Ga. Code Ann. ss. 24-3-17, 35-3-34 (1989), etc.). In yet other States, a general exemption is provided explicitly for computerized public records of public agencies (e.g. Virginia - Va. Code Ann. s. 8.01-391 (1989), Oregon - Or. Rev. Stat. s. 192.005 (1989)).

For those local governments claiming proprietary interests in their GIS digital files and the products generated from them (i.e. those local governments that are selling or licensing GIS data sets or access to them), government records exceptions to the hearsay rule may not be available. In these instances, the argument may be made that the government has a significant "private" interest in the records, the records do not constitute "public records" within the meaning of the statutory exception because they lack the requisite assurances of trustworthiness, and the computerized records should be inadmissible unless allowed by some other exception (such as the business records exception).

3. Additional Means of Admitting GIS Evidence

If all else fails and a computer generated record is inadmissible due to failure to meet a hearsay exception or failure to meet authentication requirements, it may sometimes enter the courtroom as demonstrative evidence. Demonstrative evidence is tangible evidence used only for explanatory purposes. Evidence developed specifically for trial in order to aid the trier of fact (i.e. jury) in understanding the testimony would be treated as demonstrative evidence. Because it doesn't have some direct or circumstantial tie to the event at issue it is not considered "real evidence." Thus, it is not formally introduced as evidence at trial nor would it typically be allowed in a jury room. Demonstrative evidence may not be "...presented solely for dramatic effect or emotional appeal" and judges retain great discretion regarding its use (Lynch and Brenson 1989, p. 934).

In addition, computer generated evidence not otherwise admitted may be admitted in some jurisdictions for limited purposes if relied upon by an expert witness. The data or printout is then admitted only for the limited purpose of showing the basis for the expert's opinion and not for the purpose of showing the truth of the data on the printout (Henak, p.58).

In Scenario 3 presented above, the GIS records of the local city government would typically be categorized by judges as "real evidence." Those records are directly germane to showing what actions the local government administrators did or did not take in their manipulation of their GIS. By contrast, it may be argued that the GIS evidence offered by the citizens group goes only to supporting an opinion of what the citizens group believes the administrators must have done to arrive at the results they did. If the judge were to hold that their GIS evidence is supportive only of an opinion and doesn't directly or circumstantially relate to the actual actions of the city administrators, the GIS products of the citizens group would be "demonstrative evidence" only. As such, their GIS analysis results would not be admitted as evidence of the truth of the matters asserted. Instead, the citizens group likely would need to first state in court the conclusions they had reached from their analysis and then present their demonstrative evidence as an adjunct to the testimony in order to show the basis upon which their opinions were reached. For complex analyses such as that described, an expert in use of GIS would typically be employed to present the conclusions and explain any underlying reasoning in the analyses
processes. Recall that whether such evidence is held to be real or demonstrative, the trial judges decision on the matter is unlikely to be second guessed by a higher court.

Although as a general rule, the rules for admissibility of computer generated evidence seem to be more burdensome than for many other forms of evidence, an anomaly seems to currently exist with regard to photographic evidence. "Virtually without exception, people and courts believe that what they see in a photograph is factually true" (Guilshan 1992, p. 365). In most peoples minds, photographic evidence tends to override any other evidence that might be presented in court. The presumption seems to be that an ordinary person (i.e. one without sophisticated knowledge and without a considerable investment in specialized equipment) would be incapable of fabricating or altering a photograph without detection. As a result, the rules for admissibility of photographs have tended to become more lenient over time. However, the assumption that photographs may typically be accepted as an unbiased reflection of truth is being severely challenged by the widespread availability of desktop image processing systems. Even those with only a casual bias against what appears or doesn't appear in a picture or image, now have the capability of altering that image or fabricating objects within a scene with minimal chance of detection. (Guilshan 1992)

Courts have tended to follow one of two primary tests for authenticating photographic evidence (Guilshan 1992, p. 368). Guilshan states that under the "pictorial testimony theory" a sponsoring witness is required to testify that what is shown in the image is an accurate reflection of that which was observed in person. If this test is used by the court, imagery evidence such as video recordings in stores of shoplifters and images from automatic teller machines would be inadmissible in court because there is typically no witness to corroborate that the image shown is an accurate reflection of what was observed. In order to avoid such results, other courts have used a "silent witness theory" for photographs and images. Under this theory, a photographic image is considered to "visually speak for itself" and because of its high degree of trustworthiness the photograph does not require the additional testimony of a sponsoring witness. The obvious drawback of this approach is that under current technological conditions it is becoming easier and easier to alter and fabricate images with little chance of detection. Because a fabricated digital image may be readily converted to a film image, it would make little sense for the courts to develop a test for admissibility which distinguishes between photographic film images and electronic digital images.

To address the dilemma, Guilshan has suggested that under current technological circumstances courts should completely eliminate use of the "silent witness theory" of photographic admissibility and alter the "pictorial testimony theory" such that only the original human photographer should be allowed to authenticate a photograph in court. This approach seems extreme since it would practically eliminate most evidence gathered by today's automatic cameras that are in prevalent use for security purposes, whether or not used in the regular course of business. This approach would also eliminate much of the imagery typically used in constructing GIS databases (i.e. that collected by automated aerial cameras and remote sensing devices). A more sensible approach for the present would appear to be to continue use of the "pictorial testimony theory" in which any person with personal knowledge of that depicted in the photograph may testify as to its accuracy. Any more specific rules in this area should arise from the experiences of the courts as they resolve issues relevant to the admissibility of computer generated evidence on a case by case basis.

Under Scenario Four presented at the beginning of this paper, the existing precedents and principles in admitting photographic evidence suggest that both the original orthophotography and the imagery of the oil spill would likely be admitted into evidence by
the court. If there is suspicion of tampering with the images, the adjoining landowner is allowed to produce evidence that such is the case. However, as stated previously, determining whether and to what extent tampering has taken place will become more and more difficult over time as digital imaging techniques advance and become more readily available to the general public. The counter prediction is that new technological innovations will allow authentication of data sets and other documentary evidence more conclusively than we have ever been capable of achieving in the present or past.

CONCLUSIONS

General rules for the admissibility of computer generated evidence in court have been discussed within a framework of relevancy, authentication, and hearsay considerations. From a pragmatic legal perspective, digital files of spatial data and the products generated from them differ from maps and plats traditionally maintained as paper documents in several respects. The hearsay rule is almost always applied to electronic data files and the products generated from them. As a result, a hearsay exception such as the business records exception or the public records exception must generally be met for GIS generated products to be admissible in court. Authentication as a condition precedent to admissibility also tends to be more complex and difficult for computer generated products. Finally, the reliability and believability of computer generated images and analysis results may be more difficult to convey to a jury and the general public.

In this author's opinion, verifying the authenticity of GIS data in order to protect the long term viability of GIS databases is likely to require development and increased use of a variety of verification techniques imbedded within the technology itself and within the infrastructure through which GIS data sets are likely to be transferred. The various techniques currently being pursued by the commercial sector in respect to electronic data interchange (EDI) should be investigated for their possible applicability within the GIS industry. Ordering the purchase of goods and services by electronic methods is now a standard operation for many businesses. A major goal of the EDI community is to develop methods of evidencing the occurrence and content of purchase transactions such that the body of evidence gathered is sufficient for both the courts and the business community. Some of the more promising EDI techniques for ensuring that data has not been altered by other than the originator include use of trusted recordkeepers, either internal or external to the organization, and cryptographic digital signatures. Although GIS data is unusual in some of its characteristics, other of its characteristics subject it to many of the same authentication problems being encountered in other electronic database domains.

ACKNOWLEDGMENTS

This article is an expansion, rewrite, and update of "Evidentiary Admissibility and Reliability of Products Generated from GIS" which appeared in Technical Papers of ACSM/ASPRS Annual Convention, Vol. 1, 1991, pp. 197-201.

REFERENCES AND FURTHER SELECTED READINGS


