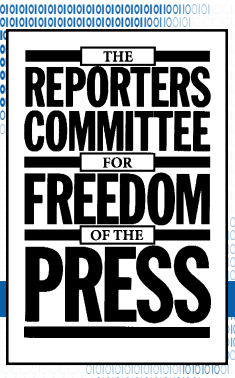
Access to Electronic Records



A state-by-state guide to obtaining government data

Spring 2003

Electronic access is critical to reporting

Reporters have a tool that allows them to report on entire populations and do original analysis on a subject for their stories, rather than relying solely on anecdotes. Computer-assisted reporting helps journalists do important stories that otherwise would not be covered.

In 1999, reporters for the *Miami Herald* used voter databases to show widespread fraud in the city's mayoral election. The series overturned the election results and won the staff the 1999 Pulitzer Prize for investigative reporting.

In 2002, *Washington Post* reporters used databases to show the District of Columbia's role in the neglect and death of 229 children in protective care. The series prompted an overhaul of the child welfare system there and earned the 2002 investigative Pulitzer.

But not all computer-assisted stories are done by large metropolitan newspapers that win Pulitzer prizes. Around the country small and medium-sized newsrooms use databases to track government corruption or systemic difficulties in a local or state agency.

But to use this tool, reporters need access to government databases. Access to electronic records often can be difficult for reporters, depending on how a particular state treats computerized information.

Prohibitive fees, privacy regulations, proprietary software and laws that don't necessarily address access to databases can be barriers to journalists acquiring electronic information.

When reporters at the *Detroit News* requested a database of driver records, they were told that it would cost about $43 million. New legislation in Michigan allows for per-record charges on driver data. In many states, access to driver data was eliminated because of state responses to the federal Driver's Privacy Protection Act.

When the *San Jose Mercury News* wanted county assessment records, it was told that a local statute allows the assessor to charge $40,000 for the database. When the *Mercury News* sought a copy of the database listing information on participants in the state's "Adopt-a-Highway" program, its request was denied because it ostensibly infringed on the participants' privacy — even though their names are already displayed on highway signs.

When a *(Harrisburg) Patriot-News* reporter tried to get records from Pennsylvania's Department of Education, the only information he could get was in PDF format on the agency's Web site. Because PDF files are difficult to put into databases, he requested another format. The agency denied the request, saying that the information was not in their possession, but rather in the hands of a vendor in Minnesota. Providing the data would take two months to prepare and cost about $7,000.

Although state governments are becoming increasingly aware of — and responsive to — changes brought by the new technologies, conflicts over electronic records access remain common.

A 2001 survey by the National Archives and Records Administration of more than 150 federal agencies and departments concluded that most federal agencies are still baffled by electronic records. According to the survey, most create documents in electronic formats, but when preserving them as official records, print them on paper and put them into storage.

"Government employees do not know how to solve the problem of electronic records — whether the electronic information they create constitutes records and, if so, what to do with the records," NARA said in a report written with help from information technology firm SRA International Inc.

In some states, government agencies contract with private companies for data processing. In some cases, because private or quasi-governmental agencies have the agencies' data, the information has not been disclosed. In other states, courts have said that if the private organization is doing government business, then the information should be public.

Is electronic information public?

A growing number of states now include electronic data in their definitions of what constitutes a public record. As government increasingly conducts its business electronically, access to computerized records becomes essential. The public must have access to electronic records or lose any meaningful way to oversee government activity. Yet agencies often resist opening their computerized records to requesters.

According to a report from the National Association of Legislative Information Technology (NALIT): "All 50 states and the District of Columbia include computerized records in their definition of public records, either specifically in the statutory language or through judicial interpretation."

Since September 11, however, some states are rethinking how they make information available. Some have curtailed the amount of information they are putting online and, in some cases, agencies have removed information.

Can a requester choose the format?

Agencies and requesters often disagree over the particular physical format — paper, tape or diskette — for delivering public records.

The format in which data are released is often as critical as the disclosure itself. A printout of raw data may be as useless to journalists as a pile of unorganized documents. One New York City department refused to provide a copy of a computer tape to a publisher. Instead, the agency proposed that the requester pay for a printout that would take five or six weeks to print, exceed one million pages in length, and cost $10,000 for paper alone.

In some cases, when raw data isn't available, news organizations must create a database from the paper documents. Because campaign finance information is not in a database in Missouri, the *St. Louis Post-Dispatch* entered the data into a computer.

How much will it cost?

The National League of Cities resolved in December 1993 that cities and towns should set higher fees for electronically stored public information to offset and recoup the costs of developing better computer systems. Since that time, many states have enacted laws or administrative regulations outlining fee structures for access to electronic records. Most states either charge "reasonable fees" or "actual costs." However, what fees agencies believe are reasonable and what may be considered an actual cost varies widely among the states.

Many officials try to recoup more than costs. These agencies try to use electronic records to generate revenue for the government's coffers. Members of the public point out that they already paid for electronic information systems through their taxes.

Is software a public record?

In most cases, reporters do not need agency software and can use just the underlying data. However, in some cases, customized software does not allow for easy data extractions. There have been disputes over whether requesters may obtain copies of specific software to read coded electronic records. Many states now address this issue in their statutes.

According to the NALIT report, state legislatures have amended their open records statutes to exempt agency-developed software. "Currently 20 states have statutes that exempt

software in some way, and the attorneys general of Michigan, Mississippi and Nevada have issued opinions exempting government software. Alaska, Florida and Kentucky specifically include software in the definition of public record."

Copyright issues arise when requesters seek some types of commercially produced software. Commercial software is privately produced and licensed to the government, and the producers believe that the government is just like any other licensee.

Some software may be prepared by a state agency or a state university. The state-created software is arguably not proprietary since it was created using state money. However, unlike the federal government, which does not copyright public information, some states claim that they may copyright items such as statutory compilations and computer programs.

In Nevada, a computer program was set up to randomly select recipients of the limited number of hunting permits issued by the state. Hunters complained that permits were not distributed fairly. But when citizens asked for a copy of the software to test how random the selections were, the Nevada attorney general advised that government-written software is not a public record.

But the Florida attorney general advised that copyrighted computer software that was licensed by a county from a private company and used for compiling county data was a public record. The opinion said the software must be made available to the public for examination and inspection only. Unauthorized reproduction of copies of the software was prohibited by federal copyright law. Since then, the Florida legislature has allowed state agencies to hold copyrights from software they develop and charge license fees for its use, so long as public access to records is not compromised.

Can government pump up the price for useful systems?

A growing number of state legislatures want to make money off of specialized computer systems called "geographic information systems. These systems manipulate large databases of information by overlaying the data on regional maps. Such GIS are tempting cash cows for municipalities because commercial organizations, such as mail order companies, are often willing to pay for access to these databases.

When reporters at *The Modesto Bee* tried to get electronic mapping files of voting precincts, the county elections office refused, offering paper or PDF files instead. The officials claimed that, because it took county workers many hours to create the files, the data should be protected work product. Unfortunately for them, California law covers this only if the government workers had created the programming language. In this case, the county used ArcView, a commercial mapping software. The reporters ended up getting the files, but got them too late to do the story for which they needed them.

Online information.

Many states provide frequently requested information on Web sites. And in some states, legal requirements mandate that some information be online.

California mandated in 1994 that all state statutes, the state constitution and current legislative information be made available on the Internet. In recent years, every state has placed varying amounts of information online. Some provide only a home page; others post statutes, case law, governmental information and agency reports online.

This guide addresses in more detail many of the issues raised earlier concerning electronic records access. In addition, the guide provides a state-by-state summary of key issues regarding electronic information.

Access to Electronic Records

Executive Director: Lucy A. Dalglish
Editors: Jennifer LaFleur and Gregg P. Leslie

Contributors: Jennifer LaFleur, Rebecca Daugherty, Kathleen Dunphy, James Getz and Alicia Upano

Funding for this publication was provided by the Robert R. McCormick-Tribune Foundation. Additional support provided by the S*outh Florida Sun-Sentinel* and *The Orlando Sentinel*

Online at www.rcfp.org/elecaccess.

The EFOIA gave promise

In 1996, the federal Freedom of Information Act was amended to specifically cover electronic information. The federal law only applies to records that are held in federal agencies, but states often imitate the federal law in passing new state legislation. The 1996 "Electronic Freedom of Information Act" also lengthened the time in which an agency must respond to FOI requests to 20 business days from 10 days. EFOIA created multiple tracks for processing requests and allows a requester to ask for "expedited processing" if a request "demonstrates a compelling need." In many cases, journalists can show that their requests demonstrate such a need.

The law, codified at 5 U.S.C. § 552, defines a record to include any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format."

EFOIA also made it clear that computer searches to retrieve records did not constitute the creation of a new record, eliminating one common barrier to reporters seeking electronic records.

EFOIA required agencies to create "electronic reading rooms" and to have a FOI Act section on their Web sites. The legislation required agencies to post online copies and indices of frequently requested records, as well as administrative opinions, policy statements and staff manuals. The provision was to be met by Nov. 1, 1997, and the requirement applied only to records created on or after Nov. 1, 1996.

While EFOIA has made it clear that electronic records are covered by the federal records law, problems still exist with agencies' EFOIA compliance.

Journalists told a House subcommittee in 2000 that agencies continued to delay requests and some failed to post frequently requested information on their Web sites.

An August 2001 report by the General Accounting Office, based primarily on federal agencies' annual FOI Act reports, found that backlogs continue and agencies need to better provide online information.

The study found a growing backlog of unprocessed requests at most agencies, while the number of requests has held steady or declined for most agencies.

Although most agencies reported that they processed simple requests within the required 20 days, other agencies reported much higher processing times.

According to the GAO report, agencies are still inconsistent in how they report their annual FOI Act results from year to year, making it difficult to look at changes over time.

For the study, the GAO also interviewed FOI Act requesters and agency FOI Act staff to study the impact of September 11 on the

FOI Act: "Agency officials characterized the effects on FOIA implementation as relatively minor. . . . In contrast, members of the requester community expressed general concern about information dissemination and access to government in light of removal of information from government Web sites after Sept. 11."

The impact of September 11 on EFOIA, however, will become clearer when annual reports covering 2002 are released.

The report found that while agencies are making efforts to put information on their Web sites, improvements are still needed: "Agencies are not devoting sufficient attention to the on-line availability of materials and ensuring that Web site content is adequately maintained, including accuracy and currency of the material and Web site links."

The Department of Justice, charged with FOI Act oversight, has made strides to implement earlier GAO recommendations outlined in a March 2001 report.

"FOIA makes government work better," said Sen. Patrick Leahy (D-Vt.), chairman of the Senate Judiciary Committee, who along with Rep. Stephen Horn (R-Calif.) requested the report.

"In times of heightened security, the tendency to close doors and conduct the government's business in secret is natural," Leahy said in a Sept. 25, 2002 statement. "Secrecy can become addictive, and that is a danger we have to guard against. The nation needs a robust FOIA in times of peace, but also in times of war. The Freedom of Information Act is the people's window on their government, showing where it is doing things right, but also where it can do better."

Horn headed the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations of the House Committee on Government Reform. Leahy and Horn were the chief authors of the EFOIA Amendments of 1996. GAO continues to examine the impact of these new FOI Act policies at Leahy's request.

May a requester choose to obtain electronic records?

A computer can search through millions of records in a relatively short period. The same task could take a reporter weeks or months of searching through paper records. So the format in which the information is produced is crucial. The requester's right to demand that information be provided in a computer printout, a computer tape, a CD-ROM or some other form varies by state — so the format can render data very useful or practically useless.

Agencies also may provide information in an electronic format that still renders it useless to a reporter. As states create searchable databases on their Web sites, reporters use them to look up individual cases, but if a reporter wants to do further analysis with the entire database, some agencies balk, saying the information is available online. In other cases, information may be available in formats such as PDF files that make analyzing them difficult.

The states deal with this issue in a variety of ways. When electronic records are sought, Oregon requires an agency to "provide copies of the public record in the form requested if available."

In California, government agencies used to be able to pick the format that they wanted to provide, but a 2001 amendment to the public records act said that requesters could get electronic files if they requested them and the agency had them in that format.

Virginia gives the agency discretion to "convert" a record to another format to satisfy a request when the document does not already exist in the requested format. The statute requires that electronic records must be "reasonably accessible."

Some statutes that do not refer specifically to electronic records require agencies to adopt "reasonable" rules and regulations regarding access and copying. It may be possible to argue that such a provision applies to a request for release of information in a specific format.

Even when an agency has discretion over the format, some courts have allowed requesters to challenge very unreasonable agency action as an abuse of that discretion. Other courts have decided that requesters have affirmative rights to obtain computer tapes or disks. In one of the earliest cases on the subject, the New Mexico Supreme Court said "the right to inspect public records should . . . carry with it the benefits arising from improved methods and techniques of recording and utilizing information contained in those records." The court ruled that political organizers had a right to a copy of a computer tape.

The Ohio Supreme Court ruled that an agency must allow copying of portions of computer tapes if the requester has presented a legitimate reason why a paper copy of the records would be insufficient or impractical.

The Georgia Court of Appeals implied that an agency cannot discriminate against future requesters when the agency provides computer tapes to one private entity. The court affirmed a deal struck by the county commissioners to supply computer tapes to a business, provided that the county did "not exclude any other individual or company from access to such records on an equal basis."

Utah agencies may not deny access because information is stored electronically. An agency must provide that information in a particular format if the agency can comply without "unreasonably interfering with the government entity's duties and responsibilities." Additional fees may be added for such a service.

The Kentucky Attorney General's Office said in an August 2002 opinion that a computer crash was no excuse for the Elsmere Police Department's decision to deny records and said that the police department's efforts to retrieve information requested under the state's Open Records Act were "inadequate." The inability of a requestor to obtain information reflects poor records management, the opinion said. "Electronic record-keeping is to enhance access, not to impede access."

Some states may permit requesters to copy electronic records with their own equipment if the agency cannot do so.

However, when a requester asked an agency to temporarily turn over original disks because the agency could not make a copy in the format requested, the Arkansas Supreme Court ruled in 1987 that the agency need provide only computer printouts. The court reasoned that a request for access to original disks was a request for equipment rather than information.

Ramifications of 9-11 Web takedowns still unclear

After Congress passed the 1996 amendments to the federal Freedom of Information Act, government agencies began putting more data and documents on their Web sites.

But after the events of September 11, 2001, several federal agencies moved to take down maps, databases and entire Web sites from the public domain, citing security reasons.

In particular, the door was shut to environmental data, transportation maps, dam locations and other databases frequently used by reporters, community groups and citizens.

Instead of the usual reports and information on Web sites, many users instead found messages saying that sites were down or information was unavailable.

The U.S. Army's Redstone Arsenal posted this message: "Due to the threat against our nation, our way of life, national security, and because I was told to do so, portions of the Team Redstone homepage have been temporarily blocked from public viewing."

Removal of information on Web sites does not, in all cases, mean that the same information will be denied a requester. Federal FOI officers can deny only information that falls within one of the nine exemptions, but agencies have been under some pressure to make information that hypothetically might be useful to terrorists less conveniently available.

One of the FOI Act's nine exemptions defers to other laws that require confidential treatment of information. In early 2003, Congress passed one law requiring the Department of Homeland Security to protect "critical infrastructure" information voluntarily submitted by businesses. It was considering additional legislation to protect information some members of Congress say would be useful to terrorists.

Since the first rush to take down federal Web sites, some of the information has been returned, but much continues to be unavailable and additional information is either being removed or not updated. In addition, proposed legislation and rulemaking could restrict information such as pipeline locations, chemical plant information and other data deemed "sensitive."

Where reporters could once get maps showing pipeline systems, the Office of Pipelines Safety Web site now has this message: "The Office of Pipeline Safety has discontinued providing open access to the National Pipeline Mapping System. Recent events have focused additional security concerns on critical infrastructure systems."

The agency went beyond just removing the information from its Web site. The information is now available only to pipeline operators and local, state and Federal government officials. Reinterpretation of FOI exemptions has allowed this to occur.

Tracking Closures

OMB Watch, a non-profit organization in Washington, D.C., concerned with freedom of information issues, has tracked federal agencies' removal of information from their Web sites since Fall 2001.

"We saw a pretty dramatic shutdown," said Sean Moulton, senior policy analyst with OMB Watch. "We haven't seen much of a reversal of that. If it didn't reverse immediately . . . it became stuck amid the debates."

In December 2001, OMB Watch sent FOI requests to federal agencies asking them to list what information they had removed from the Web sites. The responses varied. The Federal Energy Regulatory Commission refused to comply with the request, saying that the mere disclosure of such a list would be problematic. Early removal of information from the agency's Web site was based on size, meaning that documents with large file sizes were removed from the electronic reading room.

"Literally tens of thousands of documents that were "FOI-able" a year ago or that you could just go get are now exempt from FOIA with no change in FOIA and no change in court rulings," Moulton said.

Rather, the changes were based on how the exemptions are to be interpreted.

The Federal Aviation Administration responded to the OMB Watch request by saying that it had not taken anything down, Moulton said. Yet the Web site where FAA enforcement data was once available now has a message stating: "The Enforcement Information System (EIS) is not available at this time due in part to security considerations."

Moulton said that one of the most responsive agencies was the Environmental Protection Agency.

"They showed that stuff was taken down and then put back up," Moulton said.

According to Odelia Funke, chief of EPA's Policy and Program Management Branch, the agency did an inventory of databases and identified where there were security issues. In the end, much of the information was returned to the agency's site. However, access to some chemical information and direct-connect access to the agency's Envirofacts Data Warehouse remain unavailable. Direct-connect allowed users to query directly the Envirofacts database.

"Agencies that took down stuff wholesale are having difficulty deciding what to put back up," Funke said.

Moves to take down information were not isolated to federal agencies. Several states removed information from Web sites as well. Pennsylvania removed environmental data from its site. A memo to New York state agencies from James K. Kallstrom, director of the Office of Public Security, and James G. Natoli, director of the Office of State Operations, urged them to review sensitive information. New Jersey removed chemical information from its Web site.

States have made efforts to exempt terrorism meetings and homeland security agencies from state public records acts.

In Illinois, a new law exempts geographic information systems from the state's freedom of information act. In Alabama, proposed legislation in 2002, submitted by the state Department of Emergency Management, attempted to make secret state agency e-mail and meeting records if they would jeopardize agency safety. It also would have exempted from disclosure vulnerability assessments and infrastructure information for many public and government buildings.

Lawmakers have been particularly concerned about disclosing vulnerabilities that they fear could be targeted by terrorists, but secrecy carries its own danger.

In June, Sen. Christopher "Kit" Bond (D-Mo.) introduced the "Community Protection from Chemical Terrorism Act," legislation that would restrict access to chemical plant's risk management plans. Environmental reporters and citizen groups have used that information to assess the risk of chemical plants in their areas. And although the information is no longer online, it is available in EPA reading rooms around the country.

But risk management plans do not provide overly detailed information about a plant, Moulton said. "It doesn't say where it [the chemical supply] is stored, nor indicate what it is stored in."

"There is a risk when industry is not under the watchful eye of the public," Moulton said. "When you get information you can create pressure to get something fixed or changed."

In July 2001, Ralph Haurwitz and Jeff Nesmith did a series of stories in the *Austin American-Statesman* looking at pipeline safety around the country.

As a result of the series, federal agencies with pipeline oversight have increased efforts to update regulatory activities and rulemaking, Haurwitz said. In addition, the Texas Railroad Commission levied its largest fine ever against a company responsible for an accident in Abilene, Texas.

Much of the data they used, including pipeline incidents and company financial information, is still available today. But other information concerning pipelines in environmentally sensitive areas is no longer available.

"Today, if a reporter wanted to do a particular analysis dealing with these areas, it would be difficult to do it because the information is no longer public," Haurwitz said.

The potential for closure of these and other types of "critical infrastructure information" worries journalism organizations.

"I think if the government gets its way it's going to be an awful lot harder to do what we've been doing," said James Bruggers, president of the Society of Environmental Journalists and environmental reporterfor *The (Louisville) Courier-Journal*. "I'm not sure what the overall benefit is. The fact that a lot of this information has been made public has made communities safer."

Does an agency have to search for requesters' records?

When an agency wants to restrict access to information, the records custodian may say that manipulating database information is "creating" a new record, which usually is not required by law.

Others argue that "creating" a specialized record is the very essence of why databases are set up. Their primary function is to permit users to manipulate data and information.

Sometimes customized searches are required only because the agency neglected to plan its database system in a way that users could access information.

When reporters at the *St. Louis Post-Dispatch* wanted traffic ticket data from a local police agency, the police agency argued that because it had no way to separate cases, it was not required to disclose from other cases, they could not provide any of the information.

Often, statutes that regulate the practice do not require an agency to manipulate computer data for requesters, but neither do they prohibit an agency's compliance with such requests.

Some statutes appear to require agencies to make reasonable efforts to provide such data. Virginia allows an agency to "abstract or summarize information," but the agency is not required to do so.

In Minnesota, requesters can ask an agency to make a custom run of summary data, if the requester is willing to pay for it.

Idaho implies a limited right of access to "analysis, compilation and other manipulated forms of the original data produced by use of the program." Oregon permits an agency to collect fees for "summarizing, compiling or tailoring" electronic records.

Computer-savvy reporters often will offer to write the program to save an agency the trouble. This may depend on which database management system the agency uses.

Courts have split on whether agencies must manipulate data for a requester. State courts sometimes look to federal law for guidance.

In 1982, the federal appeals court in Washington, D.C., held that "an agency is not required . . . to create a document that does not exist in order to satisfy a request." *(Yeager v. Drug Enforcement Administration)*

A U.S. District Court in San Francisco (9th Cir.) ruled that an agency was not required to manipulate exempt information on personal tax returns to provide a breakdown of non-exempt information. The court ruled that the request involved "editing so extensive as to amount to the creation of new records." *(Long v. IRS)*

However, more recent federal cases impose greater burdens on federal agencies to search for specific information. A federal district court in San Francisco ruled in 1989 that an agency must search all data banks to find specific information sought. *(Mayock v. Immigration and Naturalization Service)*

The U.S. Court of Appeals in Washington, D.C., appears to have narrowed its earlier holding in *Yeager* when it found in 1994 that a publisher's FOI Act request for specialized address lists from the Health Care Financing Administration was reasonable, even though it would require a search through the agency's database.

However, the court ruled that the information, which was compiled from tax return information, was exempt from disclosure under the Revenue Code and the FOI Act's Exemption 3. *(Thompson Publishing Group, Inc. v. Health Care Financing Association)*

In an administrative decision, the U.S. Department of Energy's director of hearings and appeals decided that generating a list of documents by computer would not be creating a "new record," even though the list did not previously exist.

The federal Electronic FOI Act was enacted to guarantee that requesters would enjoy the same benefits from electronic record-keeping enjoyed by the agencies themselves. It is consistent with later developments in case law, imposing the requirement of "reasonableness" in determining whether an agency has made an adequate search through its records for requested information.

Although many states look to federal law for guidance, it remains to be seen whether the "reasonableness" standard will carry the day.

States move more records to the Internet

Increasingly, agencies are looking at ways to put government records online. All states now offer some type of information through the Internet.

In Maine, nearly all business records of the Secretary of State are available online, along with all state regulations, statutes and legislative information on the state's Web site.

California has made all state statutes, the constitution and current legislative information available in electronic form over the Internet. Many other states offer full-text legislative information through the Internet without usage fees.

In November 2002, the South Dakota Supreme Court began broadcasting live and archived arguments on the Web.

Tennessee's legislature gave a committee "exclusive authority" to approve "direct access" to the legislature's computer system, but only if "protection of any confidential information is ensured."

Florida allows any records custodian to permit "remote electronic access to public records" but permits an agency to charge special fees for access.

Many state agencies offer online access to information, although there is no specific statute that sets up the service. For example, Montana runs a legislative information service similar to California's. The main difference is that California's system is established by law. Montana's is not.

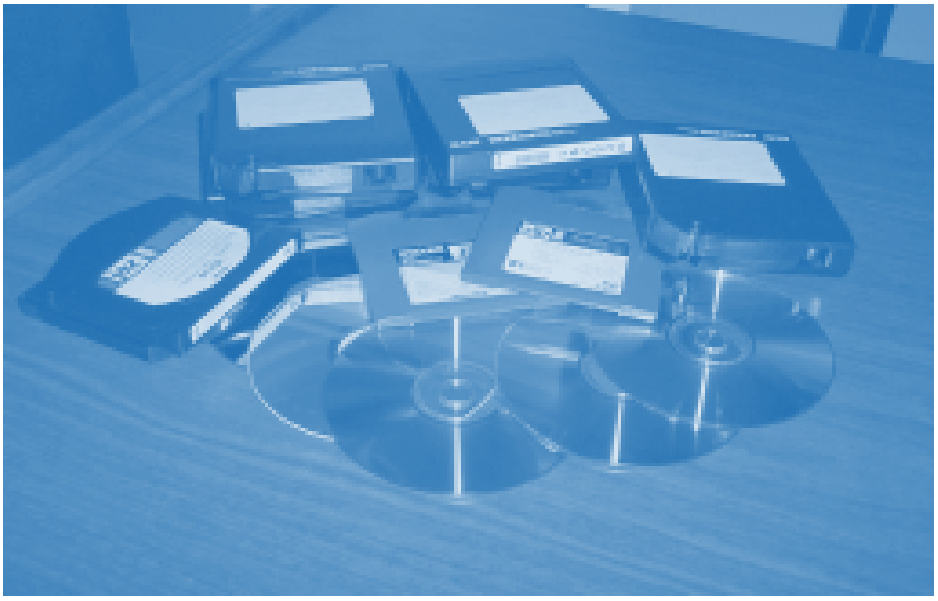
Increasingly, courts are putting information online as well. Of those that make information available electronically, some provide free Web-based services; others have fee-based services.

U.S. Supreme Court cases are available online, as are those from a variety of other jurisdictions, although the amount of material varies. The federal PACER system allows subscribers to access docket information for a fee. In some jurisdictions, the courts, in concert with law schools or universities, make opinions, orders and rules available on the Internet.

From May 2001 and June 2002, an advisory panel created by the National Center for State Courts met to study access to electronic court records and develop model guidelines to be applied to state court systems.

The Reporters Committee for Freedom of the Press released a detailed analysis of the proposed model guidelines, which is available at www.rcfp.org/courtaccess.

Is an agency's software considered a public record?



In some cases, reporters' quests for data require that they also have access to specialized software developed by or for a government agency. This can lead to problems if software is not considered a public record in that state.

Of all the answers to electronic records questions, perhaps the least consistent are rulings addressing release of software. Nearly every state allows agencies to keep information confidential if it qualifies as a "trade secret." The definition of a trade secret, however, varies from state to state and does not necessarily apply to software.

Government agencies usually acquire software in one of three ways. First, the state may purchase software from a commercial vendor.

With newer, post-Y2K computers, many government agencies are using standard database systems such as SQL server or Oracle. Second, the state may develop the software itself. Third, the state may contract with an outside party to create specialized software. Police departments often purchase specialized software for crime analysis, for example.

Most states that have chosen to regulate access to software explicitly exempt it from their public records statutes, regardless of whether it is a commercial or an agency-written program.

Minnesota permits an agency to copyright or patent a computer software program or components of a program created by that government agency to make it exempt as a trade secret.

A reporter for the Minneapolis *Star-Tribune* had to pay a $200 programming fee for county payroll data. The reporter requested a copy of the program to see if the cost was justified. The county refused on the grounds that software is not a public record. Without the program there was no way for the reporter to know if the charge was fair.

North Dakota requires agencies to copyright or patent agency-created programs before withholding them.

A few states also exempt related material. In Illinois, an agency may withhold "operating protocols, computer program abstracts, file layouts, source listings, object modules, load modules, user guides, documentation pertaining to all logical and physical design of computerized systems, employee manuals," and other information. This exemption creates a significant barrier for reporters for whom raw data is useless without the appropriate documentation.

Oregon and Idaho allow an agency to withhold computer programs, but not mathematic and statistical formulas that manipulate computer data. Such language allows public scrutiny of how the agency conducted its search where accuracy and fairness of the program might be at issue.

Mississippi takes a unique tack. It places the burden on a software supplier to get a court order prohibiting release of a program. The agency is required to notify the supplier of a request, but if the software licensor does not respond after a waiting period, the government must release the software.

Trade secrets "developed by a college or university under contract," which may include software, are exempt from disclosure altogether.

A few states limit an agency's authority to withhold software. For example, Florida allows an agency to keep software confidential only if it was "obtained by an agency under a licensing agreement which prohibits its disclosure and which software is a trade secret." The statute also exempts "sensitive software" developed by an agency.

A few statutes allow collection of additional fees for the release of some software programs developed at government expense. These statutes mimic GIS concerns about private entities receiving public "subsidies."

Minnesota permits an agency that develops software "with a significant expenditure of public funds" to charge a fee that includes a share of the "actual development costs of the information" if the software is used to access data that has commercial value.

The Texas Attorney General suggested that agencies could withhold programs on a case-by-case basis if release would pose a security risk, the programs qualify as trade secrets, or the material would be exempt from discovery in a civil lawsuit.

The Nevada Attorney General adopted a broad exclusion for computer programs by finding that they do not qualify as public records.

The attorney general's office in Florida has issued several opinions that address software issues. It considers the purpose of the software when determining whether it is a public record. One computer program developed by an agency to perform financial functions was a public record.

Another program that processed voter registration data was exempt as "sensitive" data processing software. Electronic voting software obtained under a license agreement was exempt as a trade secret. And copyrighted software obtained from a private company was available for "examination and inspection purposes only."

Data processing software is now included under Florida's definition of a public record.

DEALING FOR DATA

The 'ins and outs' of negotiating for electronic records

Just as with dealing with paper documents, getting electronic information from a government can be difficult. But following a few strategies and learning the "ins and outs" of data can help make it a little easier. Here are some things you should know when accessing electronic records:

Know the law. Know how your state treats (or doesn't treat) electronic information and what the exemptions to the open records act are.

Know what information you want. Don't ask an agency to provide you everything it has. Make sure your request is narrow and specific. Also, you don't always have to ask for the data first. Request a list of its databases. Then ask for record layouts for specific databases. Then ask for the data. One helpful tactic is to request the agency's Y2K compliance reports, which often list all databases affected. Some of that information may now be outdated, but it could be a good starting point.

Know how the information is kept. Try to find someone in the information systems department at an agency who knows how the information is kept. The public affairs officer that you usually deal with may not know the details of the databases.

Know what the appropriate cost should be. In most states, you should really have to pay only duplication costs. If they hit you with a high price, ask them to itemize the costs — frequently this request alone will decrease the fee.

Know who does the data entry. The best resource to any database are the data entry clerks.. They can tell you details about how the information is input and how often it is updated.

Know who administers the data. The persons in charge of the database can be much more helpful that the agencies' public relations persons. Sometimes they can be pretty excited to have someone take an interest in their database. Long before you ever need the data, tour the agency's data processing center — get to know the folks you need to meet. Go to software users groups — there are usually some data processing folks from government agencies there.

Get hard copy summary reports. Summary reports will help you to check your data and may give you hints about what data the agency keeps.

Know how many records or pieces of information are in the database. When you get the database, make sure you have the right number of records.

Increasingly, reporters face two major hurdles in gaining access to databases. Agencies will claim that release of data on named individuals intrudes upon their personal privacy. And agencies will try to sell public record data for profit.

It is increasingly difficult in many states to get any data on individual people — and there is little public support for access to such data. Be persistent at getting the data while it is still available and get together with other news organizations to fight impending closure of these databases.

Insist that you should only pay for reproduction costs. Neither government agencies nor outside companies who process their data should be profitting from the sale of public data. Wealthier news organizations may sometimes pay more than cost just to get the data more quickly, without challenging unfair costs. However, there is a danger that those sales set a precedent that hurts overall access to public information.

In some cases, the law does not clearly say whether you have a right to a particular database. That does not mean you should not try to get it. In fact, news organizations have done important stories with data that was not necessarily a public record. When a *Miami Herald* found voter fraud in the mayoral election, the records were not open records at that time.

The North Andover *Eagle-Tribune* in Massachusetts found public officials who were getting welfare checks by analyzing a welfare database that was leaked to them by a source.

In other cases, you may be able to argue that you are entitled to at least portions of the database. Find out whether a researcher or another government agency has ever gotten the records.

Argue that the public has an interest in the disclosure. Identify important important stories that have been done using the records you seek or similar records in other jurisdictions. Remind officials that they are accountable to the public. A politician interested in "cleaning up government" might release records. Find similar records that have been released.

Making your request

Determine whether an agency will be cooperative before using tactics that might be seen as confrontational. A records custodian may provide records you need without requiring a formal request.

If the agency makes electronic records available to other agencies, it may produce them for a requester. Many agencies now make computer terminals available for public use.

Develop a good "paper trail." As you appeal an adverse decision, good documentation of your request and the agency response will be valuable.

Show how your request is reasonable by including information you learned earlier. If state statutes support your request, cite them. If any court decisions from your state support your request, cite those as well. Alternatively, cite other state or federal cases, especially those from jurisdictions that are nearby or have public records laws similar to yours.

Address fees. Because of the potential costs of computer access, it is important to discuss fees in your request letter. Ask that the agency incur no costs until it advises you, or state the maximum you are willing to pay. Ask for fee waivers where appropriate. Offer to discuss your request with agency officials to avoid delays.

Follow up any denial with oral negotiations. Ask a records custodian if you can narrow a request to satisfy the custodian's concerns or reduce fees. Try to negotiate lower fees if necessary.

Determine if an administrative appeal is available. Some states allow, or even require, review by another public official before an appeal to a court. Explain in detail why your request is, or ought to be, covered by the state open records law and why a denial is unlawful or unreasonable.

Pursue a judicial appeal if necessary. Your case may warrant an appeal to a court. Seeking legal representation is best, but if you cannot afford an attorney, you may be able to pursue your own appeal.

All evidence you have gathered will be important at this stage. You must also address cases that weaken your position. If a case is contrary, demonstrate how your situation is different from that considered in the earlier case.

Learn to talk like a nerd

Megabytes, density, ASCII. Mention these terms and many journalists turn pale. But knowing a few computer terms can help unlock the door to a wealth of information. Suppose you were interested in investigating federal contracts granted to companies in your area.

You could examine summary reports

created in an agency office, but you might want to look at the records themselves. Imagine sorting through thousands of documents. Making sense of such information would take a *very* long time. Looking at that same information on a computer makes it easier, if you know what you're doing.

The information in your computer is a bunch of little on and off switches that form different patterns to stand for different things. Each switch is called a "bit" — that stands for Binary DigIT. It's how the computer stores information: 1 or 0, off or on, yes or no.

Information is just like your old secret decoder ring where a certain pattern would stand for a certain letter. For example, J51 might have stood for the letter A. Your computer does the same thing with different patterns of bits.

In order to have enough combinations for all the possible letters, numbers and symbols, your computer needs eight slots — that group of eight on/off switches is called a byte. That secret decoder language that your personal computer uses is called ASCII. So, for instance, the bits 01001000 make up a byte with the value of 72; the ASCII value of 72 is "H"

Another type of language is EBCDIC. That takes more work to translate, but if it is all you can get, take it.

And, for those of you who want to sound especially techno-savvy in your negotiations: ASCII stands for American Standard Code for Information Interchange and EBCDIC stands for Extended Binary Coded Decimal Interchange Code.

You also may have the opportunity to get data in a variety of formats including CD-ROM, DVD, tape cartridges, 9-track tapes and diskettes. You will need to make sure your computer can read some types of media such as 9-track tapes.

In addition to the data, you also will need some hard-copy information. You must have a record layout — that is the map to your data. You also need to know some format information about the data.

Once you have determined if your file is ASCII or EBCDIC (or is one of those rare files already in a database or spreadsheet), you need to know if the information is arranged in fixed or delimited fields.

A fixed length file has everything in columns; delimited files typically have commas separating each piece of data, so your database or spreadsheet program knows which piece to put into the first column, second column and so on.

With this information, you can import the information into a spreadsheet or database program and, using your record layout information, start compiling useful information from what started as a bunch of computerized bits.

Overcoming common excuses

The previous guidelines are all dandy, until you actually ask for the data. Many times you will run into excuses. Reporters may, more often than not, just accept the excuses agencies give them for keeping the data to themselves. But often sheer persistence will pay off.

Our database is too complicated

Knowing the lingo will pay off. If you understand databases and the officials can see that - you will have more success getting a database.

Our computer system can't output a file

It would be unusual for this statement to be true, but it does happen. If you can't find someone at the agency who can figure out how to export the data, find out what software they use. You might have to call a vendor directly to get information on exporting from its software.

Some reporters run into cases where an agency uses software with which they are familiar and can talk the agency through the exporting process.

The person who knows how to do that is on vacation for two weeks /doesn't work here anymore.

If you are not willing to wait, you may have to find another tactic. Does another agency keep the same data? Could the agency's software vendor help you? If they realize that you are not going to go away, they may be more willing to work with you.

It will cost you $20,000

Know the law and how fees can be assessed in your state. Ask for an itemized estimate of charges. Find out what it really costs agencies to reproduce the data.

Offer to pay reasonable programming fees. In most states, you should only have to pay the programmers their hourly rate, not overhead.

If they do programming, ask for a copy of the program or at least have them put in writing that they will save the program in case you need the data again next year. See if there is a rate charged by state agencies to other agencies. Provide your own tapes, disks or CDs. Ask for a backup tape.

In some cases, this actually might be the price charged to that agency from a larger state data processing center. For example, in California many agencies are charged such fees from the Teale Data Center.

The database is not public record.

The burden is on the agency, not you, to show where in the open records law the information is exempt from disclosure. If only part of the information is exempt, most states require that they redact the confidential information, and give you the rest.

We don't like what you plan to do with it.

Most open records laws do not require that you disclose what you plan to do with the data. Some states ask reporters to complete data disclosure forms asking what the purpose of a request is. In these cases, be as vague as possible. You may not know everything you plan to do with the data.

We don't keep that on computer.

Make sure that is true. If you have a computer-generated report from the agency, the agency probably does keep the underlying data on its computer. However, you may actually run into cases where records are not computerized. In that case, you may want to have a data entry firm input the information or enter it yourself. Some journalists scan data, but scanning numbers can introduce errors into your data. For instance, it is very easy for a "2" to become a "7" in the scanning process.

That uses proprietary software.

You do not want the software, you want the data. If agencies do not know how to copy to a file or print to a file, find out who their vendor is.

We don't mind giving you a few records, we just don't want to give you the whole database.

When the *San Jose Mercury News* sued for a pet license database, the judge asked the agency's attorney: "You mean if they wanted ONE record from ONE person it would be okay?" The attorney answered: "Depends on the person." The *Mercury News* lost the suit on a finding that disclosure would invade pet owners' privacy. However, in most states, if one record is a public record, all of them should be.

Privacy laws block database access

Electronic records are subject to the same exemptions from disclosure under open records laws as paper records.

Some agencies maintain that there is a greater risk of invasion of privacy if personally identifiable information is easily retrieved from computers. Legislators are beginning to scrutinize traditionally public records, worried that their disclosure intrudes upon privacy.

The argument by these agencies that computerized records are somehow more intrusive on personal privacy than paper records is a dangerous one and has led to serious losses of important news stories.

Privacy advocates have convinced some legislators that personally identifying information in databases should be withheld. This can render the data useless because the reporter has no way of distinguishing one person from another.

For reporters who wish to match two databases – to learn, for instance, if teachers within a school system are convicted child molesters, or if ambulance drivers have been convicted of drunken driving – denials of identifying details can be devastating. Without personal identifiers such as name and date of birth such analyses are virtually impossible.

Driver records, voter records, hunting licenses and personnel records have all been vulnerable to privacy protection in recent years. Even databases as innocuous as pet licenses have been withheld on privacy grounds.

Concerns over personal privacy have caused some courts to resist releasing computerized information. These cases often involve commercial requesters who want names for mailing lists or sales prospects.

A California Court of Appeal cited concern for "extensive dissemination" of juror questionnaires "with the ubiquitous availability of integrated computer information circulating freely." The court prohibited the distribution of the information for privacy reasons.

Even where the same computer information would later be published in a public directory, the Michigan Supreme Court wrote that providing a computer tape containing the names and addresses of students at a state university "was a more serious invasion of privacy than disclosure in a directory form" because "computer information is readily accessible and easily manipulated."

The 3-3 deadlock among justices in that case let stand a lower court decision denying public access to the tape.

A dissenting justice in that case wrote that "we cannot accept the conclusion that the Legislature intended to allow a public body to exempt otherwise public records by the simple expedient of converting the public record from one form to another."

Other courts have overruled similar privacy arguments. The New Mexico Supreme Court held that release of computer tapes does not create special privacy concerns.

Minnesota and Illinois courts have also repudiated privacy arguments in cases seeking lists of doctors who performed state-funded abortions.

If some material in a record is confidential, a principle accepted by the federal government and most states requires agencies to delete that material and provide the remainder to any requester.

This process traditionally involved a records custodian drawing a black line through an entry in a paper document. But some software is not designed to automatically redact confidential information from electronic records.

Several states have recognized the need to separate confidential and public information at the time the data are entered into the computer systems, not down the road when a member of the public requests the record.

The Ohio Supreme Court ruled that a public officer has a duty to maintain files in a way that allows confidential material to be deleted and the remainder provided to the public "within a reasonable time."

When privacy concerns required a school district to delete names and other identifying information and then "scramble" the alphabetized record to further protect identities, the Illinois Supreme Court said such manipulation would not be "overly burdensome."

On the federal level, Justice Anthony Kennedy, while serving as a judge on the U.S. Court of Appeals in San Francisco (9th Cir.), wrote in *Long v. U.S. Internal Revenue Service* that deleting names and addresses from tax files would not be overly burdensome. 596 F.2d 362 (9th Cir. 1979), *cert. denied*, 446 U.S. 917 (1980).

That order, he found, would not violate the court-imposed rule that an agency is not required to create a "new record" in response to an FOI Act request.

Reporters need to argue strenuously against the categorical application of privacy exemptions in open records laws.

Passage of censorial privacy protection laws must be curtailed. Congress passed the Driver's Privacy Protection Act in 1994 to protect personal information in driver records. Rep. Barbara Boxer (D-Calif.) hoped to prevent stalking when she introduced the measure, but it has stopped reporting that relied on driver records in all 50 states and the District of Columbia.

Medical privacy regulations developed by the Department of Health and Human Services in response to a congressional mandate similarly will bar news stories that need to be told. The regulations go into effect in April 2003. And yearly, state and federal legislatures suggest new ways to bar use of information in overzealous attempts to address exaggerated privacy concerns. ◆

Agencies move data processing to private firms

Across the country, government agencies contract with private organizations to carry out tasks that would normally be governmental functions. But because those organizations are private, they are not always bound by state public records laws. Depending upon the state, open records laws may apply if the organization is supported by public money or performs a public function.

The Press-Enterprise in Riverside, Calif., sued late in 2001 to obtain an employee roster and salary data from a corporation formed in a joint venture by a hospital district to run the district's facilities. But the superior court ruled that the language of the state open meetings act applied only to "nonprofit" boards in this situation. In 2002, the public records law in California was amended to include nonprofit or for-profit corporations whose boards are subject to the open meeting law.

A Texas appeals court in Waco ruled in 1998 that the Brazos Higher Education Authority, Inc., a nonprofit corporation that issues revenue bonds to purchase student loans, is not a governmental body under the public records act.

In 1996, the New Mexico Foundation for Open Government sued Corrections Corporation of America for access to inmate records at the Sante Fe Juvenile Detention Center, which the company operates. An eventual settlement determined that the records are subject to New Mexico's Public Records Act, Arrest Records Information Act, Children's Code and other state open-access laws. It also said the company served as a "custodian of public records" as defined in the Public Records Act.

When a reporter for the *Lexington Herald-Leader* requested property data from several counties, they were told that the counties contract with a private vendor that would charge $500 per county and an additional $500 per town within the counties. The newspaper regularly acquires similar data from the city of Lexington for about $20.

A Kentucky appellate court ruled in1996 that the control of a private entity by a government official does not necessarily convert the entity's records into public records.

Quasi-governmental agencies

In California, much of the data processing done for state agencies is done by the Teale Data Center. When agencies attempt to provide data that is at Teale, they are charged processing costs, which they pass on to requesters.

In St. Louis, the Regional Justice Infor-

mation Service was created through a joint agreement between St. Louis and St. Louis County to provide data processing for law enforcement and court information. When the *St. Louis Post-Dispatch* requested data housed at REJIS, reporters were told that the organization was not bound by the open records law, but they did offer to do a special data run for the newspaper for a significant fee.

In Missouri, quasi-public government bodies do not include urban redevelopment corporations, which are privately owned, operated for profit, and do not expend public funds. Such urban redevelopment corporations are not subject to the Sunshine Law.

A Florida appellate court in Daytona Beach ruled in 1999 that a local chapter of the humane society was subject to the state's open records laws because of its status as a quasi-public agency.

Statutes

State law varies in how it treats these organizations. In Alaska, records that are "developed or received . . . by a public contractor for a public agency" are "public records" available for inspection and copying.

The Tennessee Supreme Court ruled in 2001 that private companies now performing functions once done by the state must open their books to the public. This ruling came after *The (Memphis) Commercial Appeal* sought the records of a private company that provided state day-care services.

The Arkansas Freedom of Information Act applies to meetings of the governing bodies of private organizations "supported wholly or in part by public funds or expending public funds." But in 1990, a court ruled that the mere receipt of public funds is not sufficient to bring a private entity within the FOIA; rather, the question is whether the private group carries on "public business" or is otherwise intertwined with the activities of government.

Many states follow the same rules as Arkansas and require that an organization receive public funds or carry out a government function to be bound by the public records law. In Kentucky, public officials must constitute the majority of the members of a private organization for it to be covered by the state's open records law.

State courts have ruled in often divergent ways on this issue, but most states back access, according to a 2000 study by the *Florida State University Law Review* and more recent court decisions. Of the 34 states that have dealt with this issue either judicially or legislatively, more than 20 have opted for an approach that favors access to records held by private companies while 11 have adopted a more restrictive attitude.

North Carolina, Oregon, Kansas and Florida have used "functional equivalency" approaches similar to Tennessee's.

In an Ohio decision, the state's supreme court said a private consulting company hired by the city of Cincinnati to choose a safety director had to release the names of job candidates. Even though the company declared the list a trade secret, the court held that, if a company carries out a public function, its records are subject to release.

Courts in other states, such as Pennsylvania and New Jersey, have held that private companies need to reveal their records only if they were formed under a state statute or in some way determined by the state to be subject to open access laws. ◆

Is a government official's e-mail a public record?

growing number of decisions and statutes directly address whether electronic mail qualifies as a public record. In a few cases, e-mail communication is also an issue with regard to state open meetings laws because business is conducted via e-mail.

In Florida, e-mail messages made or received by a state agency in connection with the transaction of official business are public records. The same holds true in Arizona, Arkansas, Colorado, Maryland and Ohio. Arguments also may be raised that many states' expanded definitions of public records now contain e-mail within their scope.

However, in Michigan, the lack of a specific statute has allowed two agencies to develop radically different e-mail practices. The University of Michigan has made e-mail private to the "fullest extent permitted by law." Washtenaw County, where the university's Ann Arbor campus is located, adopted a resolution to make county government e-mail open to public scrutiny.

The conflicting policies in Michigan illustrate the tensions between open records laws and privacy concerns. Open records advocates argue that e-mail is a natural product of the move toward "paperless" offices. Others argue that government employees use e-mail believing that the messages are private.

In December 2002, a circuit judge in Fredericksburg, Va., ruled that a group of officials violated the state's open meetings law when they e-mailed each other regarding city business.

The Connecticut Freedom of Information Commission has proposed restrictions on use of e-mail. If the new rules are adopted, a majority of a board's members would not be allowed to discuss the same subject using e-mail, because it would constitute an illegal meeting and thus exclude the public. The commission intended to reach a decision by Spring 2003.

The Florida Attorney General found that "the use of an electronic bulletin board by water management district basic board members to discuss matters that may foreseeably come before the basin board over an extended period of days or weeks, which does not permit the public to participate online, is a violation" of the state's open meetings law. But the attorney general also has said that "a school board may use electronic media technology in order for a physically absent member to attend a public meeting of the board if a quorum of the members is physically present."

It is not clear in all states whether open records laws apply to e-mail such as intra-office memos, letters from citizen-taxpayers, and government employee correspondence from an outside bulletin board.

On the federal level, the U.S. Court of Appeals in Washington, D.C., held that substantive e-mail communications are records under the Federal Records Act. The Federal Records Act covers the preservation of the transaction records produced by federal agencies. In *Armstrong v. Executive Office of the President*, the court ordered periodic review of electronic record-keeping practices at the National Security Council.

A federal district court in Tennessee ruled that a media plaintiff had no First Amendment right to city government employees' Web browser history and "cookie" files, which store information about Web sites the user has visited. The court noted that it did not address whether the files would be available under the state Public Records Act. *(The Putnam Pit, Inc. v City of Cookeville)*

Fees assessed in varying ways from state to state

The size of fees an agency charges for access to electronic data are critical to many requesters. Arbitrary and prohibitively high fees can undercut a requester's ability to utilize freedom of information laws. There are nearly as many approaches to fees as there are states. Fees for computer time, programming time, printouts, supplies, labor and overhead may be assessed against the requester.

Many states have just started to address fee schedules for electronic records access. Texas was one of the first states to outline charges for databases. The Texas General Service Commission established suggested charges for diskettes and fees for access time on various types of computers.

Many statutes state that an agency may not charge more than "actual cost." Connecticut requires that fees for a "printout of transcription . . . shall not exceed the cost thereof to the public agency."

Some states allow additional fees for computer records. For instance, Indiana law permits an agency to charge "the standard cost, if any, for selling the same information in the form of a publication." When accessing the Indiana legislative services agency, a requester may be charged "a reasonable percentage of the agency's direct cost of maintaining the system in which the information is stored."

Some statutes prohibit agencies from charging for the time to search electronically stored documents. Others say agencies may assess a fee for that service. States also split on whether agencies may or must grant fee waivers to reporters or other requesters when disclosure is in the public interest.

The market value of disclosed electronic government records should have no bearing on their cost to the public, which has already paid for gathering and storing requested information. Fiscally strapped agencies may see the sale of government information as a means of generating revenue.

In a few states, journalists are running into agencies that want to charge them "commercial" fees. Commercial requesters are treated differently in some states.

Reporters for *The Daily Oklahoman* ran into this problem when they asked the county assessor for copies of his property assessment and sales data and plat maps. The assessor argued that because the newspaper also does database marketing and direct mail marketing for paying clients, he could charge the full commercial rate for the data unless they only asked for specific data planned for use in a specific story. He also argued that keeping the data after the specific story ran would make it a commercial use.

But Oklahoma's records law makes a distinction between "commercial" requests for records and "public good" requests: "Publication in a newspaper or by broadcast news media for news purposes shall not constitute a resale or use of data for trade or commercial purpose and charges for a news purpose shall not exceed the direct cost of making the copy."

Because agencies sometimes assess inflated costs for computer time, requesters may want to question high charges. The National Institute for Computer-Assisted Reporting, based at the University of Missouri, suggests that a requester who is charged by the minute should multiply the per-minute charge claimed by the agency by the 525,600 minutes in a year and compare the result to the actual yearly expense the agency pays for operating the computer services. Also, if an agency is charging for programming time, find out what the salary for the programmer is to see if it is charging a fair fee.

Requesters should refer to the statutes, official regulations and informal policies of each office if they have questions about fees agencies charge.

To sign or not to sign: Use caution with predisclosure forms

Many reporters trying to get data are faced with requirements from agencies that they fill out a predisclosure agreement stating why they want access to the data. This is a common practice with health and science data. Some agencies have such forms on their Web sites. Before data can be downloaded, reporters must complete the form.

In the Winter 2003 issue of *News Media and the Law*, published by The Reporters Committee for Freedom of the Press, three media attorneys addressed the issue of predisclosure forms. The following are excerpts from the attorneys' responses on this issue.

David B. Smallman, Steinhart & Falconer LLP, New York, N.Y. The extent to which reporters should explain the basis for document or data requests and their intended use of the materials depends upon the applicable law and the factual circumstances. Practical considerations may affect technical rights under access laws. And reporters may be asked to consent to limitations of their rights, for example through terms of use agreements on government Web sites.

The devil is in the details.

As a general matter, the federal freedom of information law and many similar state laws do not require disclosure of the purpose for the request. However, access laws typically create practical incentives for reporters to disclose their status, which can result in expedited consideration of their requests and result in fees that are reduced or waived. Representatives of the news media and others can seek a fee waiver under the federal FOI law. Doing so, however, may require disclosures about why the information is of public interest, the name of the news organization, information about expected publication, and whether the release of information will "contribute significantly to public understanding of government operations and activities." Similarly, expedited review requests may require detailed disclosures about the public's "urgent need" for information in a specific context.

While access usually is available to "any person" who "reasonably describes" the information sought, some states, such as Pennsylvania, restrict the right to inspect and copy records to citizens of the state. For sensitive undercover or investigative stories, keep in mind that your requests may create a paper or electronic trail.

Another important consideration arises if access to information is conditioned upon a voluntary agreement by the reporter that effectively waives certain First Amendment or other rights. Reporters' agreements have been held by courts to be subject to *promissory estoppel* law, which essentially imposes an obligation on those making promises to keep them. While this issue often arises in connection with agreements between reporters and confidential sources, it also can apply to situations in which reporters agree to "security review" when covering military, police or intelligence-related stories.

Because consent to certain conditions before gaining access to government data may impose restrictions inconsistent with constitutional, statutory or common law rights, carefully review terms of use agreements on Web sites before agreeing or clicking through. Consider whether the conditions imposed may later come back to haunt you and ask yourself if there is some other way to get the data. Consult media counsel for specific language if the option of modifying the terms of use is presented. Subsequent challenges to improper terms of use agreements, while possible, can be expensive and the results uncertain.

Recent passage of the E-Government Act of 2002 suggests that a proliferation

of online regulations (and end-user agreements) affecting security, privacy and confidentiality may be on the way, so increased vigilance by journalists is warranted.

Tom Clyde, Dow, Lohnes & Albertson, Atlanta, Ga. At both the state and federal level, it is becoming common for government agencies to ask that public records requests be submitted in writing, often on a preprinted form that requests an explanation of what you plan to do with the information. The general rule under both federal and state freedom of information laws is that your purpose for requesting information is irrelevant to an agency's duty to provide it.

So, is this just improper snooping? Frequently it is, and the agency's request for an explanation can be ignored. But there are exceptions to this rule. Sometimes an agency is legally entitled to enough information to determine whether you fall into a certain category of record requesters, such as commercial requesters, who may be entitled to less information or who may be required to pay a higher fee.

In the area of health care information, federal privacy regulations now impose a duty on agencies to identify requesters and their purpose in order to determine if identifiable patient information may be disclosed.

In making a record request, the first question to consider is whether you submit a written record at all. As a practical matter, it often is to your advantage to do so. At federal agencies, until a record request is submitted in writing, the Freedom of Information Act does not apply. So a federal agency may provide records in response to an informal verbal request, but it is not legally required to do so.

At the state level, state freedom of information laws vary on the issue of whether a records request must be in writing to trigger the state's disclosure requirements. For example, Maryland, Michigan and New York require written requests; Colorado, Florida and Georgia permit verbal requests.

Even if not legally required, however, having a written record of the request is frequently critical in the event the agency resists or delays disclosure, and you have to try to compel compliance through an administrative review or court action. But keep in mind that government officials may more easily review written records requests in attempting to anticipate and blunt future investigative stories.

In competitive markets, where more than one news organization is chasing the same story, reporters sometimes review an agency's records request log to see what their competition is up to.

Given these concerns, it is generally advisable to keep any explanation of your intended purpose for requesting information to a minimum. As mentioned above, under the federal Freedom of Information Act and most state freedom of information laws, the purpose for which information is sought generally is irrelevant, so providing even a general explanation is not legally required.

There are some exceptions to this rule, however. Many state records laws prevent or limit access to certain information, particularly personally identifiable information, if it is sought for a commercial purpose.

Particularly in the area of health care information, the government does have a reason for asking who you are and generally what you plan to do with information. Under federal privacy regulations scheduled to go into effect in April 2003, agencies are under an affirmative duty to monitor their disclosure of any information containing individually identifiable patient information. Under the regulations, agencies can release individually identifiable information to certain relatives and organizations such as hospitals and law enforcement agencies, but must otherwise "de-identify" the data prior to release. Accordingly, if your request includes patient identifying information, a brief disclosure that you are seeking information for news reporting on health care matters should assist the agency in determining the appropriate level of disclosure and undertaking the "de-identification" process.

James Chadwick, Gray Carey, Palo Alto, Calif. Whether you should complete a form that requires you to say why you want information depends on the open records law you are using. For the federal government, the Freedom of Information Act generally applies. Each state has its own laws, which typically apply to both state and local governments, and some cities and counties have their own special laws. Individual government agencies often have their own specialized regulations.

Under the federal FOIA, the purpose for which a request is made is generally irrelevant to whether you are entitled to the information you are requesting. However, you may need to confirm that you are a journalist in order to avoid having to pay for the costs of document search and review.

In addition, under the FOIA you may need to provide information about the federal government activity you are investigating and why you have an urgent need to report on it to the public if you want to get expedited processing of your request. Be careful. Such requests frequently are denied, even when they have merit.

Many state open records laws are the same. For example, California's Public Records Act expressly states that limitations on access are not allowed based on the purpose for which a record is being requested.

That being said, in at least two situations you may need to provide at least some description of your purpose for seeking the records.

First, some statutes expressly limit the release of information to those who are going to use it for certain purposes, typically "scholarly or journalistic" purposes. If the information you are requesting is governed by such a statute, you may have to explain that you are a journalist and that you are seeking the information for purposes of news reporting.

In regards to information that is for release to "researchers," I think a reporter can make such a claim, if it is done in a way that is not misleading. The reporter should make it clear that they are a journalist and not a scientist, but can legitimately say that the media frequently engages in sophisticated analysis of data for the purposes of reporting to the public, and is seeking the information for that purpose.

Second, the information you are requesting may be exempt from disclosure. Agencies sometimes provide access to exempt information even though they are not expressly required to do so. In this situation, the agency can pretty much define the terms upon which it releases information, and you may have to complete a form or answer questions about your purpose.

Finally, the basic rule for what you say about your purpose is: the less the better. Say only as much as you need to in order to get access. Start with a generic description, such as: "For purposes of news reporting."

This may be sufficient in some circumstances, particularly if the statute permits disclosure for journalistic purposes. If the agency tells you that you have to provide more information, and the records are important, you can elaborate.

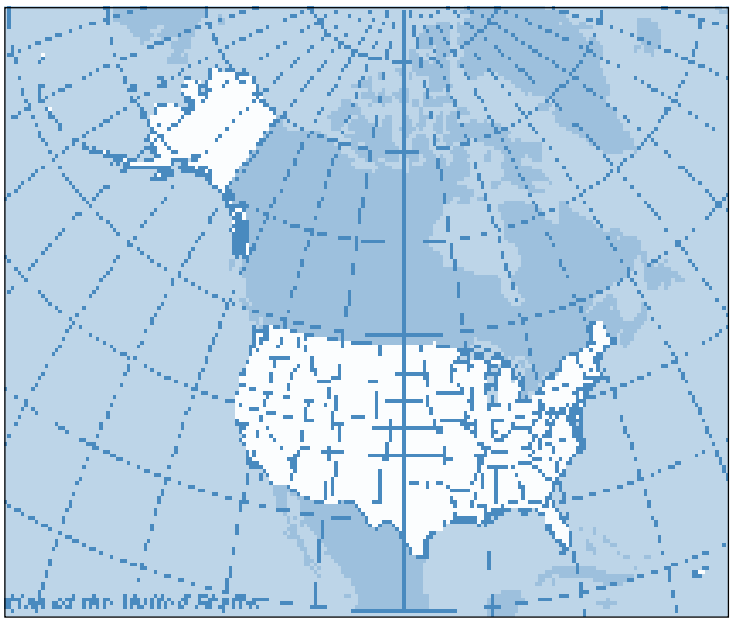
Keep three things in mind if you complete a form to get records.

First, you probably are signing an agreement. Could you have problems if you violate it? Make sure you read what the form says about the information you are providing. For example, does it require you to sign under penalty of perjury? What limitations, if any, does it impose on what you can do with the records you get? Are there consequences for violating the agreement, such as criminal prosecution?

Second, be careful about signing a form that imposes limitations on your access to or use of information that are not justified by the law. Agencies may try to get you to sign such forms, even though you are entitled to the records without having to do so.

Third, you may later want to invoke the reporter's privilege if someone tries to make you testify about your sources or unpublished information you obtained during your investigation. You may not be protected with respect to information you have provided to the government, if it comes out.

Some states plot access to maps



Around the United States, police departments, county planning agencies and other government agencies are developing extensive systems to apply their data to maps. Computer systems called geographic information systems, or GIS, give agencies the power to do complex mapping.

The Chicago Police Department uses GIS to track neighborhood crime. St. Louis uses mapping to study redevelopment and plot census data. Some of these agencies make maps available online. Some government agencies charge large sums of money for actual copies of GIS data because they are valuable to real estate companies, developers and marketing firms.

The substantive conflicts over GIS access involve fees and the desire of governmental bodies to turn these systems into cash cows.

Agencies argue they have created an "added value" to these systems that justifies the greater access fees, by creating the maps themselves, such as the boundaries of voting precincts or city council wards.

The Ohio Attorney General opined that if "the Department of Natural Resources stores, produces, organizes, or compiles public records in such a manner that enhances the value of data or information included therein, it may charge for copies an amount that includes the additional costs of copying the information in such enhanced or 'value-added' format."

Another barrier to GIS information came After September 11, when many agencies decided that making mapping data public could leave them vulnerable to terrorist attacks. On the federal front, maps showing pipeline locations, water supplies and nuclear power plants were no longer available to the public because of national security concerns.

States also are looking at legislation that could limit access to GIS data. In Illinois, a senate bill exempting computer geographic system information from the state's freedom of information act became law in July 2002.

A majority of states have GIS laws on the books. The statutes appear in scattered sections of each state's code.

Some GIS laws, such as Arizona's, are codified in the public lands code. Alaska's GIS law is included in the code containing the civil procedure rules.

Florida's law is included in the section on communications and data processing. California includes rules governing disclosure of mapping records in its open records law.

Maryland's GIS law tries to strike a balance between the financial interests of government and the desire of the public for open access. The systems, which are developed with public funds, "should not be unreasonably withheld from private commercial users." However, GIS "should not provide a public subsidy to private commercial users."

A Maryland agency may sell a GIS database "for a fee that reasonably reflects the cost of creating, developing and reproducing the product."

The agency may reduce or waive fees for products and services used for a "public purpose."

The Supervisor of Public Records in Massachusetts addressed this issue of GIS and money-making in a 1996 opinion: "The temptation for public officials to increase revenue by sale of valuable information, such as that contained in a GIS database, is understandable.

However, the premise behind the Public Records Law, and other open government laws on the federal and state level, is that the public has an absolute right to access public information held by the government. The public should not be required to pay a premium for access to information which it has already paid to create and maintain through taxes."

Index to state laws on electronic records