SPRING 2000 | VOLUME 2 | NO. 1

NYSBA

Government, Law and Policy Journal

Editorial Office
GLP Journal
Government Law Center
Albany Law School
80 New Scotland Avenue
Albany, NY 12208
518.445.2329

Send Address Changes to:
Records Department
New York State Bar Association
One Elk Street
Albany, New York 12207
518.463.3200
nysba.org

***GLP Journal* Production**
Wendy Pike

Contents

 ISSN 1530-3942. The *GLP Journal* is published twice a year.

Message from the Chair

Welcome to the second edition of the *Government, Law and Policy Journal*, which is proof positive of the commitment of the New York State Bar Association's continued focus on the unique needs of government and non profit agency attorneys. This past year has been one filled with significant milestones for our Committee on Attorneys in Public Service.

- The first *Government, Law and Policy Journal* was distributed in November and focused on Ethics issues. I am pleased to report it was a huge success and has been garnering praise throughout New York State.
- Our Committee's 2000 Annual Meeting CLE program on "Is the Supreme Court Changing the Balance of Power? The Sovereign Immunity Cases," proved exceedingly timely in light of the recent Supreme Court decision. Committee Member Marge McCoy of the Court of Appeals was instrumental in suggesting Professor Chemerinsky, Sydney M. Irmas Professor of Public Interest Law, Legal Ethics and Political Science, University of Southern California Law School, a nationally renowned author and lecturer on the topic of Sovereign Immunity. I thank Marge for her insights in identifying this topic and for her assistance with this program, and Professor Chemerinsky for providing a thought-provoking seminar for our participants.
- Our First Annual Award for Excellence in Public Service was presented to Judge Joseph Bellacosa at the annual meeting in January. Patricia Bucklin not only worked on the First Annual Award for Excellence along with Rachel Kretser and Robert Smith, but she lent a personal touch to the evening and the presentation, making it all the more meaningful for Judge Bellacosa. Many thanks to Patricia. I am advised that our awards ceremony and networking reception provided NYSBA members with an opportunity to meet many of New York's finest jurists and dignitaries who attended to honor Judge Bellacosa. I thank Hank Greenberg for stepping in at the last minute to act as Master of Ceremonies due to my illness. From all accounts, a good time was had by all.
- Our Committee web site is up and running, so please visit us under NYSBA's committee web sites at **www.nysba.org**. Committee Member Michael Moran has done a spectacular job in his initial design of the web site, and welcomes your input so that we can build a viable interactive web site. In this edition of the *GLP Journal* we ask for your feedback and help, so that we can better serve your needs and interests, and properly reflect the concerns of all Public Service Attorneys.

The Committee is looking forward to continuing the momentum with this second edition of the GLP *Journal*. As you may recall, this is a collaborative effort, as the Committee works with the Albany Law School's Government Law Center, headed by the ever dynamic and indefatigable Patty Salkin, in conjunction with Rose Mary Bailly and Professor Vin Bonventre. The quality of this publication is as a direct result of the hard work of these individuals with the Editorial Board and authors of the various articles. I strongly encourage those of you reading this edition to come forward with ideas for the next edition of the *Government, Law and Policy Journal*.

As we now go to press in the Spring of 2000, Committee Member Tyrone Butler's CLE program on Administrative Adjudication is about to be held in three locations throughout the state. This is another first for the Committee, and we are grateful to Tyrone and his colleagues for their efforts in producing this program, and also to NYSBA's CLE Committee and CLE Director Terry Brooks for their support in sponsoring this excellent seminar. Many attorneys in public service in the past indicated that more targeted MCLE programs would greatly enhance their NYSBA membership, and this collaboration is further proof of the Association's commitment to addressing our needs.

Each of these endeavors epitomizes the spirit of public service attorneys. Team work and cooperation were apparent in all aspects.

On a personal note, this past year was a time of change and some turbulent periods. I held three positions within one year, all of which were in government service. Throughout these changes I knew that I could rely upon the members of the committee to step in to assure that this Committee's mission stays in focus. I would like to thank all of the members of the Committee who have worked tirelessly to make certain that the mission does not flounder, a special thanks to my Vice-chair Hank Greenberg and our NYSBA Staff Liaison Pat Wood for their attention to detail and follow through.

Let's continue the GLC and other successful partnerships focusing on government lawyers within the New York State Bar Association and all bar organizations. With your help we can continue to use our voice effectively to represent all Attorneys in Public Service.

Tricia Troy Alden
Chair of the Committee on
Attorneys in Public Service

Tricia Troy Alden is Vice President-General Counsel & Secretary for The Long Island Rail Road Company. She formerly served on the Attorney General's Executive Staff as Assistant Attorney General in Charge of Recruitment and Legal Education and later as an Assistant County Attorney for Suffolk County.

The Committee on Attorneys in Public Service Promotes Excellence and Provides Services to the Public Bar

By Henry M. Greenberg

The Committee on Attorneys in Public Service took center stage at the 2000 Annual Meeting of the New York State Bar Association this past January in New York City.

The Committee sponsored a well-attended continuing legal education ("CLE") program on recent U.S. Supreme Court decisions expanding the sovereign immunity of state governments and challenging the power of the federal government. Presented by the nationally recognized constitutional scholar and Supreme Court commentator, Erwin Chemerinsky, the program was tailored to meet the unique needs of government attorneys and received rave reviews.

Also during the Annual Meeting, the Committee gave its first annual "Award for Excellence in Public Service" to Judge Joseph W. Bellacosa. The reception for Judge Bellacosa—who will soon retire from the Court of Appeals to become Dean of St. John's Law School—drew a veritable "Who's Who" of the bench and bar with close to 200 in attendance. The event epitomized everything our Committee seeks to accomplish. Here's why.

The mission of the Committee—pure and simple—is to advance the interests of attorneys in public service. To that end, the Committee created the Award to honor attorneys who have committed themselves to the highest and noblest calling afforded by our profession: to preserve and protect the public.

To be sure, recipients of the Award must distinguish themselves in public service. But the Award honors more than professional success. The Committee seeks to recognize an individual who embodies Louis Brandeis' vision of government attorneys being "the People's lawyers." The Award, therefore, is given to an attorney whose career bespeaks a passion for justice and a singular commitment to the public interest.

These are the values the Committee promotes through the Award—values exemplified by Judge Bellacosa. Throughout more than 30 years in public service Judge Bellacosa has demonstrated an abiding commitment to doing the public good. Since 1987 he has sat on the Court of Appeals, and before that served as Chief Administrative Judge of all New York State courts (1985-1987), Chair of the New York State Sentencing Guidelines Committee (1983-1985), Chief Clerk and Counsel of the Court of Appeals (1975-1983), Law Secretary to a former Presiding Justice of the Appellate Division, Second Department, and Professor of Law and Assistant Dean at St. John's University School of Law (1970-1975). Simply put, if you think of a career as a work of art, Judge Bellacosa has painted a masterpiece!

Winston Churchill once said that you make a living by what you get, but you make a life by what you give. Over his long and distinguished career, Judge Bellacosa has given, and given, and given. By making him the first recipient of the Award for Excellence in Public Service, the Committee honors not only him, but also an ideal to which all of us can aspire.

The Committee has not rested on its laurels since the Annual Meeting. This Spring, for example, the Committee sponsored a CLE program in Albany, Buffalo, and New York City focusing on the prosecution and judging of administrative hearings. This program represented the only practice-oriented CLE offering of its kind available to attorneys in New York State.

As you can see, the Committee has been extremely busy, and the best is yet to come. Indeed, over the next several months we plan on announcing a number of new initiatives designed to promote excellence and provide services to the public bar. Stay tuned!

Henry M. Greenberg, Vice-chair of the NYSBA Committee on Attorneys in Public Service, is General Counsel to the New York State Department of Health. His previous government positions include law clerk to Chief Judge Judith Kaye and Assistant U.S. Attorney, Northern District New York.

NYSBA 2000 Annual Meeting Highlights

The NYSBA Attorneys in Public Service Committee sponsored two events at the 2000 Annual Meeting. The first was an MCLE program, "Is the Supreme Court Changing the Balance of Power? The Sovereign Immunity Cases," presented by Professor Erwin Chemerinsky, a professor from the USC Law School. The program was chaired by Committee Member, Marge McCoy.

The educational event was followed by the Committee's presentation of its first Award for Excellence in Public Service. The recipient was Court of Appeals Judge Joseph Bellacosa. He was honored for his three decades of extraordinary contributions as a public service attorney. Over 150 NYSBA colleagues and members of the judiciary attended the reception.

NYSBA President Thomas Rice shares personal perspectives on the Judge's selection as the award recipient. Hank Greenberg, Committee vice chair, and Pat Bucklin, Awards Committee co-chair, also spoke at the event.

NYSBA President Tom Rice presents the Award for Excellence in Public Service to Judge Joseph Bellacosa

Judge Joseph Bellacosa

Marge McCoy

Erwin Chemerinsky

Editor's Foreword

Vincent M. Bonventre

Technology and public service attorneys. A potent combination with profound implications. Perhaps nothing else will have so enormous an impact on the development and direction of the law in the foreseeable future as the confluence of these two forces. It thus seems especially fitting that this first issue of the *GLP Journal* in the (putative?) new millennium be devoted to the legal uses—and abuses—and ramifications of the role of technological innovations in government.

Response to the inaugural issue of this *Journal* was enthusiastically positive. Ethical questions confronting government attorneys were explored in a diverse collection of articles that readers evidently agreed underscored and illuminated the significance of the topic. We have good reason to hope that readers will similarly find this current issue to be interesting, enlightening, and provocative.

Certainly, the legal and policy questions that arise out of the intersection of government and technology are as compelling as they are ubiquitous and vexatious. A sampling of the most salient of technology's promise and problems is presented in the varied selections here. As in *GLP*'s first issue, the articles offered here are intended to be not only edifying, but also readable, accessible, enjoyable, and where appropriate, lively. We believe our readers will find that the contents of this issue fit that bill.

Introductory comments cum warnings by Fred Provorny, the head of Albany Law School's Science and Technology Center, note that no aspect of the public sector is untouched by the "possibilities and pitfalls" of rapidly changing technology. In an article authored with Brenda Stadel, Provorny then turns his eye to the European Union's efforts to protect private information. The co-authors examine the rather comprehensive provisions in the "EU Directive" dealing with the collection and dissemination of personal data, and contrast these European regulations to the limited protections variously found in American statute and common law. In a related article, Gina Marie Stevens takes a look at some specific responses taken by the federal government to the proliferation of electronic, online information and the attendant threats to personal privacy. Michael Moran considers a twist on the theme: personal misuse of the Internet and e-mail by individual employees, and preventive measures, both legal and technical, available to organizations to address this growing concern.

Rose Mary Bailly

Robert Freeman looks at New York's Freedom of Information Law and the ways in which the revolution in information technology has necessarily revolutionized the availability of government records to the public, and concomitantly, the precautions needed to guarantee security. Peter Reinharz, Barry Steinhardt and David Kaye provide a mini-symposium on governmental collection, storage and dissemination of DNA data. Reinharz applauds the benefits to law enforcement; Steinhardt decries yet another government intrusion on individual privacy; and Kaye tries his hand at balancing competing constitutional interests.

James Natoli directs our attention to geographic information systems, i.e., "computerized mapping [and] much more." He discusses the uses and implications of this powerful tool for a wide range of public endeavors, from community planning to law enforcement. Amy Vance reports on a pilot program in New York that permits the use of fax and electronic filing of court papers; reductions in cost and time, and increase in accessibility are expected. In his essay on Internet resources for the legal practitioner, Kirk Lewis reviews the searchable data bases he has found valuable in supplementing a limited traditional library. Lastly, Donald Berens analyzes four ethical questions arising from the increased presence of new technology in the work of government employees; two are hypothetical, two real, all four implicate New York's Public Officers Law.

A journal such as this is obviously not possible without the special efforts of several individuals and the good collaboration of many more. Collectively, of course, our authors are responsible for the content of this issue. Individually, credit for this issue belongs foremost to Associate Editor Rose Mary Bailly. She took primary responsibility for the solicitation and selection of manuscripts, for the completion of editorial preparations, and for the coordination of duties and organization of materials. Everything good about this issue benefited from her hands-on role in the entire editorial process.

(Continued on page 17)

Introduction: The Technological Revolution in Government

By Frederick A. Provorny

The technological revolution epitomized by the mushrooming use of the Internet has had a profound impact on state and local governments. At the National Governors' Association meeting held at the end of February 2000, it became apparent that state government is investing billions of dollars in technology this year in a frenetic effort to keep up with the new information-based economy.[1] *New York Times* correspondent Thomas Friedman struck a responsive chord with the assembled state chief executives when he told them, "If the United States of America doesn't become as efficient as America Online, government will become irrelevant."[2] Given the direction in which governments at all levels is heading, it is indispensable that lawyers in the public sector become familiar with, and responsive to, the sea changes that new technology will engender.

From paying taxes over the Internet, online automobile registration, voting by computer, "smart cards" containing a person's complete medical history, "virtual" trials and appeals in litigation and other developments once considered in the realm of science fiction, government—and governance—as we know it is changing rapidly. There is no aspect of public life—from law enforcement and administration of criminal justice, to economic development—that can hide from it. People are becoming increasingly comfortable with computers and the Internet, are getting accustomed to reading about breakthroughs in the diagnosis and treatment of disease, and expect their governments to adapt to these advances. However, concern mounts about security, privacy of personal information, crime on the information superhighway, and the impact of technology on our democratic institutions. The recent publicity about hackers breaking into popular Web sites and shutting them down has increased pressure on governments at all levels to make these issues high priorities. The fact that some of the most notorious hackers come from outside the United States causes many to seek a worldwide solution to these thorny problems. This is an area in which governments will be perceived as having a special responsibility to work in collaboration with the private sector.

The articles in this issue reflect some of the possibilities and pitfalls with which government lawyers must be concerned in the 21st century. Three articles are about the involuntary collection and retention of DNA samples from persons arrested for crimes. Society will have to balance the benefits of having a large DNA database which can be used either to identify hitherto undetected criminals or to exonerate those wrongfully convicted with the potential that the genetic information so obtained can be used for purposes other than those of legitimate law enforcement. Two articles involve new technologies that will revolutionize the ways in which geographic information will be analyzed and used and justice will be administered. Other articles involve consideration of novel challenges to employers emanating from providing employees with access to the Internet and E-mail in the workplace, as well as the tension between maintaining privacy of information and the impact of technology on the public disclosure of government records in the contexts of the New York Freedom of Information Law, the Internet and the relative protection afforded personal information in the European Union and the United States. Finally, one article deals with complex and troublesome problems of government ethics occasioned by the conflicts that may arise from public employment and the commercialization of technology and the concomitant inducements to entrepreneurship.

These articles thus provide a smattering of the virtually endless array of issues that will confront government lawyers as they navigate the uncharted waters of the new technological age. But navigate them they must. The Chair of the National Governors' Association, Gov. Michael Leavitt of Utah, put it this way: "States can fight the changes and die, accept them and survive, or lead and prosper."[3]

New York is fortunate to have many institutions that are poised to make the state a leader in the technology revolution. One that is especially well suited to assisting government lawyers and policymakers is the Science and Technology Law Center[SM] at Albany Law School. At the core of the Center's mission is working closely with the state and local governments in dealing with issues such as those featured in these articles and conducting research and educational programs into ways to use the legal system to make the state more competitive but protect the values that make the United States the envy of the rest of the world. For all of us committed to serving the public, the trip into this new territory may be disorienting at times, but the rewards of more efficient, responsive and useful government will be breathtaking.

Endnotes

1. *See* Robert Tanner, *Governors Pour Billions into Internet Technology,* Albany Times Union, Feb. 28, 2000, at A1, col. 5.
2. *Id.* at A6, col. 2.
3. *Id.* at A6, col. 3.

Frederick A. Provorny is the Director of the Science and Technology Center of Albany Law School. He also holds the Harold R. Tyler Chair in Law and Technology.

Protection of Personal Privacy Information in the European Union and the United States

By Frederick A. Provorny and Brenda M. Stadel

Introduction

For many years there has been a tension between the needs of individuals to keep personal information private and legitimate needs of public and private entities for such information. Personal information may include names and addresses; buying habits; personal preferences; and health, credit and employment records. Such information can be very valuable to businesses and government entities, not only for direct marketing purposes but also for business development, market analysis and the targeting of various social services.[1] As discussed below, in the United States protection is limited to discrete types of information rather than to personal privacy in general. In many cases protection is restricted to personal information held by government entities rather than the private sector[2] and some statutes which purport to protect privacy in the private sector actually do the reverse.[3]

The advance of technology has made it increasingly easy to collect and disseminate information about private individuals.[4] Private government databases are increasingly being networked. Often information is collected without the knowledge or control of the individuals ("data subjects").[5] As a result, without appropriate protection for data subjects, information may be collected, disseminated without knowledge or permission and misused.[6] An additional problem is the maintenance and dissemination of inaccurate information, particularly when the information is used to make decisions about a particular data subject, without the data subject's knowledge that the data exist or are inaccurate.[7]

Another factor which has assisted the collecting, processing and dissemination of personal information is the use of national identification numbers, such as social security numbers in the United States. Such numbers, although developed for public purposes, have effectively evolved into keys to sets of personal information. As a result, an individual's social security number may be used to obtain vast amounts of that individual's personal information.[8]

The European Union (EU) has recognized the importance of protective personal privacy without unduly hindering the collection and dissemination of valuable data within the Member States. In response to personal privacy concerns, the EU has adopted Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data ("EU Directive").[9] The most significant provisions of the EU Directive will be described below.

In the United States, statutory protection of personal privacy has been offered only with respect to specific aspects of particular issues, such as credit and banking, medical records, and tax records.[10] There is also federal legislation protecting the privacy of electronic communications.[11]

Of the various protections provided, most concern the confidentiality of particular types of records rather than the right to correct inaccurate information. However, the Fair Credit Reporting Act[12] is an example of legislation which allows for the review and correction of data by the data subject. There has been no blanket protection such as that provided in the EU to give individuals rights to object to the dissemination of their personal information or to correct information collected about them. There is also a limited degree of personal privacy protection under common law theories of defamation, invasion of privacy and implied contract.[13]

The adoption of the EU Directive has already affected businesses and governmental entities in the United States.[14] For instance, advocates of personal privacy protection in the United States support the adoption of standards equivalent to those in the EU Directive.[15] Businesses not only oppose the adoption of legislation modeled after the EU Directive, but have expressed concerns about the effect of the directive on their ability to gather information they perceive is necessary.[16]

An exhaustive comparison of the EU Directive with the specific statutory protection provided under state and federal law is beyond the scope of this article. However, this article will examine the most significant

provisions of the EU Directive and will consider the federal Fair Credit Reporting Act;[17] and the New York Personal Privacy Protection Law[18] and the Freedom of Information Law.[19]

The EU Directive

The EU Directive was adopted to protect two competing interests: the free movement of data within the Member States of the EU and the personal privacy of individuals.[20] The free movement of data within the Member States would occur through the standardization of their respective national laws regulating database privacy.[21] The privacy of individuals would be protected by limiting the purposes for which data may be collected and disseminated;[22] providing for regulatory oversight by Member States; and conferring enforcement rights upon data subjects. The data subjects must be notified upon the collection or dissemination of personal data,[23] may object to the processing of personal data,[24] and may sue for damages.[25] In addition, the EU Directive requires protection of the confidentiality and integrity of the data.[26]

The scope of the EU Directive is very broad, except that it does not apply to matters which are outside the scope of EU law and those which concern public security, defense, State Security and criminal law; and purely personal or household activities.[27] The EU Directive applies to ". . . the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which forms part of a filing system or are intended to form part of a filing system."[28] Processing includes any type of ". . . operation or set of operations which is performed upon personal data . . ."[29] Examples of processing include, but are not limited to, the collection, storage and dissemination of data.[30] The controller of the data ". . . determines the purposes and means of the processing of personal data . . ." and may be a natural or legal person, public authority, agency or body.[31] The controller may designate a processor to complete the actual processing.[32]

Personal data include ". . . any information relating to an identified or identifiable natural person ('data subject') . . ."[33] "[A]n identified person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[34]

Furthermore, the EU Directive applies to the governmental units of Member States as well as to the private sector. It also applies to the institutions of the EU, even though by its terms it would appear not to apply.[35]

Member States are required to provide by legislation that personal data must be (1) processed fairly and lawfully; (2) collected for specified, explicit and legitimate purpose; (3) adequate, relevant and not excessive considering the purposes for which the data is collected; (4) accurate and if necessary kept up to date; and (5) traceable to particular data subjects for no longer than is necessary.[36] Member States must also provide that data may be processed only under one of the following circumstances: with the unambiguous consent of the data subject;[37] when processing is necessary for the performance of a contact to which the data subject is party or to take preliminary steps requested by the data subject prior to contracting; to satisfy a legal obligation to which the controller is subject; to protect vital interests of the data subject; to perform a task in the public interest or exercise of official authority of the controller or third party to whom the data are disclosed; or where processing is necessary for legitimate interests of the controller or third party to whom the data are disclosed.[38] Although this last exception could swallow the rule if read expansively, processing data for purposes of the legitimate interests of the controller or third party is not permitted where such interests are overridden by the data subject's fundamental rights and freedoms.[39] Member States are also required to determine more specifically the conditions under which a national identification number or other identifier of general application may be processed[40] and under which processing of data, in general, will be considered lawful.[41]

With exceptions, Member States are required to prohibit ". . . processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[42] The exceptions are numerous and include, for example: processing with the explicit consent[43] of the data subjects except where the laws of Member States do not allow consent to override the prohibition; processing to meet obligations and rights of the controller with respect to employment law; and where it is necessary to protect the vital interests of the data subject or another person when the data subject is physically or legally incapable of giving consent.[44]

Member States must also provide for one or more public authorities to act as supervisory authorities in monitoring the application of the legislation implementing the directive.[45] The responsibility to monitor requires direct oversight over the processing of data. For instance, before processing data, controllers must provide notification to the supervisory authority.[46] Member States are required to identify those operations which are likely to ". . . present specific risks to the rights and freedoms of data subjects" and to examine those operations before the processing.[47] In addition,

Member States must provide for the publication of processing operations and require the supervising authority to keep a register of processing operations for which it has received notifications.[48]

The rights provided to private individuals under the directive also serve to regulate database creation, maintenance and dissemination. For instance, whether the information is collected from individuals directly or from other sources, individuals have certain notification rights. Regardless of how the data are collected, data subjects must be notified of the identity of the controller and representatives of the controller; the purposes of the processing; the recipients or categories of recipients; and the right to access and correct the data.[49] If the information is collected directly from the data subjects, they must also be notified as to whether replies to questions are required or optional as well as the consequences for failure to reply.[50] If the information is not collected from the data subjects directly, they must also be notified of the categories of data that will be collected.[51] If data are not collected from the individual directly, the individual has the right to notification at the time of the recording of the data, or if the information is to be disclosed to a third party, at the time of such disclosure.[52]

Individuals are also given the right to access the databases regarding their personal information and to request correction of inaccurate information. Individuals may also object to their personal information being processed for the purposes of direct marketing.[53] The notification given to data subjects from whom data are not collected is therefore essential in allowing individuals to exercise control over their personal information. In addition, Member States are required to enact provisions requiring that personal data be accurate and, if necessary, kept up to date using every reasonable step.[54]

The EU Directive also prohibits the transfer of data to a third country which does not ensure an adequate level of protection.[55] Whether protection is adequate is determined based upon ". . . the circumstances surrounding a data transfer operation or set of data."[56] Consideration is given to the nature of the data; the purpose and duration of the processing; the countries of original and final destination; the laws of the country of destination; and the professional rules and security measures followed within the destination country.[57] The provisions are of particular concern to U.S. businesses because the laws of the United States and of the included states may not meet the standards of the EU Directive for the export of data.[58]

Finally, the provisions of the EU Directive are enforceable only upon the implementation of national laws by Member States;[59] or as to those provisions which are sufficiently precise and unconditional as against Member States only upon the expiration of the Member State's deadline to adopt implementing legislation.[60] The EU Directive by itself, however, does not authorize private individuals and entities to enforce the provisions of the EU Directive against each other. Therefore, the enabling legislation of each Member State is necessary to provide full protection to the private sector.[61] It is also possible, given the discretion afforded Member States, that there may be slight differences between the Member States.

Fair Credit Reporting Act

The Fair Credit Reporting Act[62] provides consumers with certain protections against the misuse of their credit histories. These protections include disclosure of consumer credit reports only in certain specified situations,[63] prohibition of disclosure of medical information on credit reports unless the consumer consents,[64] rights of consumers to obtain a copy of their credit reports,[65] rights of consumers to correct inaccurate information on their credit reports,[66] and limits on the data that can be provided on a credit report.[67]

Credit reports may only be disclosed to persons other than the particular consumer in accordance with a court order, under written instructions of the consumer directing disclosure, to child support collection agencies in certain instances, or for certain specified purposes.[68] Such specified purposes include where the credit reporting agency has reason to believe the information will be used for employment purposes; for underwriting insurance for the consumer; in relation to a credit transaction involving the consumer; for determining the eligibility of the consumer for a license or other benefit granted by a governmental entity which is required to consider the applicant's financial responsibility or status; by a potential investor or insurer with respect to valuation or assessment of the credit of prepayment risks of an existing credit obligation; or for a legitimate business need regarding a business transaction initiated by the consumer or to review an existing account for compliance with the terms of the account.[69]

Disclosures of consumer credit reports for employment purposes are subject to conditions. For instance, before disclosing a consumer credit report for employment purposes, the consumer must be notified that a credit report will be obtained and must authorize the disclosure of the report.[70] If action adverse to the consumer is taken upon the report, the employer must provide the consumer with a copy of the consumer report and a description of the consumer's rights under the Fair Credit Reporting Act.

Consumers also have certain rights with regard to unsolicited credit or insurance transactions. In such

instances, a report may be disclosed only if the consumer authorizes disclosure or the transaction involves a firm offer of credit or insurance and the consumer has not made an election to have his or her name removed from lists of names provided by the credit reporting agency.[71]

The Fair Credit Reporting Act may be enforced by the Federal Trade Commission and certain other federal agencies and states.[72] Consumers may also bring suit against anyone who willfully[73] or negligently[74] fails to comply with the Act. In both cases, the consumer may be awarded actual damages and reasonable attorneys fees. However, for willful failure to comply, the consumer may also be awarded punitive damages.[75]

Many of the protections provided under the Fair Credit Reporting Act are similar to those provided in the EU Directive. However, credit reporting agencies are not required to notify a governmental agency upon each dissemination of data and there are no specific requirements for credit reporting agencies to protect the security of the data.

Personal Privacy Protection Law in New York

In addition to various statutes requiring confidentiality of personal information collected by state agencies, such as tax information, the Public Officers Law provides for personal privacy protection under Article 6 and Article 6-A.

Personal Privacy Protection Law

Article 6-A of the Public Officers Law, entitled Personal Privacy Protection Law, provides that State agencies retain "only personal information which is relevant and necessary to accomplish the purposes of the agency required to be accomplished by statute or executive order, or implement a program specifically authorized by law."[76] An exception is made for unsolicited personal information.[77] Agencies are also required, among other things, to maintain the data so that decisions about the data subject may be made with accuracy, relevance and completeness; collect information directly from the data subject whenever possible; establish appropriate safeguards to ensure the security of the records; provide notification to data subjects from which they request information from; and provide disclosure of the information to the data subjects under certain circumstances.[78] The notification must include the name of the agency along with any subdivision of the agency which is requesting the personal information; the name and contact information for the agency official responsible for the records; the authority under which the information is collected; the principal purpose for collecting the information; and the uses which will be made of the information. The Public Officers Law also provides a procedure by which data subjects may request correction their personal information from state agencies which hold such information.[79]

Disclosure of personal information may be made only under specified circumstances.[80] Most of the circumstances relate to inter or intra governmental transfers of information. However, disclosure may also be made pursuant to the written consent of the data subject, court order, statute, or search warrant; as well as pursuant to FOIL provided that such disclosure would not constitute an unwarranted invasion of personal privacy.[81]

Data subjects who are aggrieved by an agency action under Article 6-A may commence an Article 78 proceeding and recover reasonable attorney fees and disbursements reasonably incurred.[82] Data subjects have the burden of proof that the agency lacked a reasonable basis for the action under dispute.[83] The right to commence an Article 78 proceeding does not, however, affect a data subject's right to obtain judicial review or relief in any other form or upon any other basis which would be otherwise available to the data subject.[84]

Freedom of Information Law

Under the Freedom of Information Law (FOIL), Article 6 of the Public Officers Law,[85] the Legislature and agencies of the state have obligations to disclose records unless the records fall within an exemption. One such exemption applies to records for which disclosure would constitute an unwarranted violation of personal privacy.[86] An unwarranted invasion of privacy is not specifically defined. However, examples include, but are not limited to: disclosure of records of patients of medical facilities; employment records such as medical, employment, credit histories or personal records; records of a personal nature when the disclosure could result in economic or personal hardship to the person about whom it relates and the information is not relevant to the work of the agency; and information disclosed in confidence which is not relevant to the ordinary work of the agency.[87] Another example is the sale or release of lists of names and addresses for use for commercial or fund-raising purposes.[88] However, there is no invasion of privacy when the data subject consents to disclosure or requests to see copies of records relating to him; or if the identifying details are deleted.[89]

Conclusion

The United States and the individual states should provide greater protection for personal privacy. Howev-

er, whether the protections should rise to the level of those provided in the EU Directive is debatable because some of the regulations the EU Directive imposes on the database controllers may be too burdensome for application in the United States. For instance, the requirement that a database controller report every dissemination of database information to a regulatory agency may amount to excessive regulation without corresponding benefit to data subjects.

In any event, the provisions of the EU Directive prohibiting the transfer of data to third countries that do not provide adequate protection should be of concern to business and government and government entities throughout the United States. Even though it is debatable whether the protections for personal privacy in the EU Directive actually are extensive as they have been portrayed, if the EU claims that our protections are inadequate, U.S. businesses that depend on exports or are multinational in scope may be put at a competitive disadvantage with their counterparts in the EU.

Endnotes

1. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L.R. 1609 (1999).
2. *See* Gregory Shaffer, *Globalization and Socialization Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 Yale J. Int'l. Law 1 (2000).
3. *See* Bank Secrecy Act, 31 U.S.C.A. §§ 5311 *et seq.* Federal provisions regarding the protection of personal information in state motor vehicle records contain provisions which purportedly would protect personal information which has been released to the private sector. 18 U.S.C.A. § 2721. Such information may only be disclosed for permitted uses. *Id.* For instance, in lieu of consent, personal information may be disclosed "[f]or use in the normal course of business by a legitimate business" to verify the accuracy of information submitted to the business by the individual; or to correct information "for the purposes of preventing fraud by, pursuing legal remedies against or recovering a debt or security interest against, the individual." *Id.* § 2721(b)(3). Personal information may also be disclosed to any requestor with the express consent of the individual. 18 U.S.C.A. § 2721(b)(13). Disclosed personal information may be sold or redisclosed by recipients only for permitted uses, other than those allowed under 18 U.S.C.A. §§ 2721(b)(11) and (12) which were amended under on October 9, 1999 to require express consent. *See id.* § 2721(c); *see* Pub. L. 106-69, 113 Stat. 986, §§ 350(c) and (d). The uses permitted by 18 U.S.C.A. §§ 2721(b)(11) and (12) include disclosure of individual records; or bulk distribution for surveys, marketing or solicitation, respectively. Individual records disclosed under 18 U.S.C.A. § 2721(b)(11) may be freely sold or redisclosed by recipients without limitation. Records disclosed under 18 U.S.C. § 2721(b)(12) may be redisclosed or sold only for further bulk distribution for surveys, marketing or solicitation. As a result, individuals who consent to the release of their personal information may find their information sold continually for marketing purposes without their knowledge or control.
4. *See* Domingo R. Tan, *Personal Privacy Protection in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 Loy. L.A. Int'l & Comp. L.J. 661 (1999).
5. David Rair and Rene Chinen, *The Consumer Privacy Debate*, 3 Haw. B.J. 34 (1999). The risk of information being collected; and used or disseminated without the knowledge of the data of subject is particular great with the use of the Internet. Schwartz, *supra* n. 1.
6. *See generally* Schwartz, *supra* note 1.
7. *See id.*
8. *See* William H. Minor, *Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections*, 28 Colum. J.L. & Soc. Probs. 253 (Winter 1995).
9. Parliament and Council Directive 95/46/ED of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) p. 0031-0050 [hereinafter EU Directive].
10. *See e.g.,* 12 U.S.C.A. § 3401 *et seq.* (limits on government access to financial records) and 26 U.S.C.A. § 6103 (privacy of tax records).
11. *See* 18 U.S.C.A. §§ 2510-2521, 2701-2711 (1998). For a more detailed discussion of this legislation, *see* Tan, *supra* note 4.
12. 15 U.S.C.A. §§ 1681 *et seq.*
13. *See* Rair, *supra* note 5.
14. *See* Shaffer, *supra* note 2.
15. *See id.*
16. *See id.*
17. 16 U.S.C.A. §§ 1681a *et seq.*
18. Pub. Off. Law, Art. 6-A (1999).
19. *See id.* at Art. 6.
20. EU Directive, cls. 2 and 3. *See also* Shaffer, *supra* note 2 at 12.
21. It must be noted, however, that the degree of uniformity amongst Member States is limited to the extent that Member States have been given discretion in the directive to further develop standards and to the extent that Member States adopt legislation which is consistent with the directive.
22. *See* EU Directive, Art. 7.
23. *See id.* Art. 10, 11.
24. *See id.* at Art. 14.
25. *See id.* at Art. 23.
26. *See id.* Art. 6(d), 16, 17.
27. *See id.* at Art. 3(2).
28. *Id.* at Art. 3(1).
29. *Id.* at Art. 2(b).
30. *See id.*
31. *Id.*
32. *Id.*
33. *Id.* at Art. 2(a).
34. *Id.*
35. At the time of adoption, the Commission and the Council publicly declared that they would comply with the principles contained in the EU Directive. In addition, Article 286 of the Amsterdam Treaty required the application of the EU directive to EU institutions and bodies. Explanatory Note, Proposal for A Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by the Institutions and Bodies of the Community and on the Free Movement of Such Data, 99/0153(COD) (Brussels, 14.7.1999).
36. EU Directive Art. 6.
37. The EU Directive does not define the term "legitimate interests." A broad interpretation of this term could likely undermine the

personal privacy protection afforded by the Act while a narrow interpretation may unduly hinder businesses.

38. EU Directive, Art. 7.
39. *See id.*
40. *See id.* Art. 8.
41. *See id.* Art. 5.
42. *Id.* Art. 8.
43. *See id.* A data subject's consent is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." *Id.* Article 2(h).
44. *See id.*
45. EU Directive, Art. 28.
46. *See id.* Art. 18. However, Member States are permitted to provide for the simplification of notification ". . . for categories of processing operations which are unlikely . . . to adversely affect the rights and freedoms of data subjects . . ." or where the controller appoints a personal data protection official. EU Directive, Article 18(2). A personal data protection official must independently ensure the internal application of the provisions of the EU Directive and keep the register of processing operations containing information required by Article 21(2). *Id.* In the United Kingdom, for instance, the Secretary of State may by Order allow a data controller to appoint a data protection supervisor subject to conditions as may be contained in such order. Data Protection Act 1998, s. 23.
47. *See* EU Directive, Art. 20.
48. *See id.*
49. *See id.* Art. 10, 11.
50. *See id.* Art. 10.
51. *See id.* Art. 11.
52. *See id.* Art. 11.
53. *See id.* Art. 14.
54. *See id.* Art. 6(1)(d).
55. *See id.* Art. 25.
56. *Id.*
57. *See id.*
58. Shaffer, *supra* note 2 at 21-46. Shaffer discusses whether the current U.S. laws meet the standards of the EU directive and negotiations between EU and U.S. officials to resolve these matters. U.S. officials have proposed a system of self-regulation by businesses. *Id.* at 45. However, this proposal has been rejected by EU officials as inadequate. *Id.*
59. The United Kingdom, for example, has implemented the EU Directive with the adoption of the Data Protection Act of 1998.
60. Such enforceability is referred to as vertical direct effectiveness and applies to those portions of a directive which are sufficient, precise and unconditional. *E.g.*, Case 8/81, *Becker v. Finanzmt Munster Innestadt*, [1982] ECR 53, [1982] CMLR 499. Vertical direct effectiveness operates as an estoppel to prevent a Member State from benefiting from its failure to implement directives.
61. However, although individuals and private entities may not enforce provisions of the directive against other individuals and private entities, such aggrieved parties may file a *Francovich* claim against the Member State to collect damages. Cases 6/90 & 9/90, *Francovich v. Italy*, [1991] ECR I-5357, [1997] 2 CMLR 66.
62. 15 U.S.C.A. §§ 1681a *et seq.*
63. 15 U.S.C.A. § 1681b(a).
64. 15 U.S.C.A. § 1681b(g).
65. 15 U.S.C.A. § 1681(h).
66. 15 U.S.C.A. § 1681(i).
67. 15 U.S.C.A. § 1681(c).
68. 15 U.S.C.A. § 1681b(a).
69. 15 U.S.C.A.
70. 15 U.S.C.A. § 1681b(b).
71. 15 U.S.C.A. § 1681b(c).
72. 15 U.S.C.A. § 1681(s).
73. 15 U.S.C.A. § 1681(n).
74. 15 U.S.C.A. § 1681(o).
75. 15 U.S.C.A. § 1681n(a)(2).
76. Pub. Off. Law § 94(1).
77. *See id.*
78. *See id.*
79. *See id.*
80. Pub. Off. Law § 96 (1999).
81. *See id.*
82. Pub. Off. Law § 97 (1999).
83. *See id.*
84. *See id.*
85. Pub. Off. Law § 85 (1999) *et seq.*
86. Pub. Off. Law § 87(2)(b) (1999).
87. *See id.*
88. *See id.*
89. Pub. Off. Law § 87(2)(c).

Frederick A. Provorny is the Director of the Science and Technology Center of Albany Law School. He also holds the Harold R. Tyler Chair in Law and Technology.

Brenda M. Stadel, Esq., is the Entrepreneurial Legal Assistance Counsel at the Science and Technology Center. She has an LL.M. in International, European and Commercial Law from the University of Sheffield in England.

Internet Privacy

By Gina Marie Stevens

It is routinely acknowledged that the success of the Internet and electronic commerce depends upon the resolution of issues related to the privacy and security of online personal information.[1] Privacy is thus thrust to the forefront of policy discussions among businesses, governments, and citizens. Threats to the privacy of personal information arise primarily as a result of the widespread increase in the availability and use of computers and computer networks, the corresponding increase in the disclosure of personal information by Internet users to Web sites, the routine collection of personal information about online users by Web sites, and the utilization of online personal information for direct marketing and advertising purposes. The Congress,[2] the executive branch,[3] courts,[4] businesses,[5] privacy advocates,[6] Web sites and Internet service providers,[7] and trade associations[8] continue to confront many issues associated with the privacy of online information.

Individuals and businesses increasingly rely upon computers and computer networks to transact business and to access the Internet. The use of computers and computer networks for personal and business transactions has resulted in the creation of vast amounts of credit and financial information, health information, tax information, employment information, business information, user information, and consumer purchase information. Online users may voluntarily disclose personally identifying information, for example, to an online service provider for registration or subscription purposes, to a Web site, to a marketer of merchandise, in a chat room, on a bulletin board, or to an e-mail recipient. Information about online users is also collected by Web sites, often without the knowledge of the user, through technology which tracks, traces and makes portraits of every interaction with the network. Web sites use "cookies" files to track information about user behavior, to understand activity levels within sites, and to build new Web applications.[9]

Technologies like data-mining software facilitate the use of online personal information for commercial purposes. Because of the power of computer networks to quickly and inexpensively compile, analyze, share, and match digitized information, electronic information is potentially much more invasive. Information that is stored electronically often can be linked by use of the same key, such as the social security number. Computers make information multi-functional as vast amounts of consumer information are collected, generated, sorted, disseminated electronically, and perhaps sold, with or without consent. How valuable the information is depends on how descriptive it is. The proliferation of online personal information, along with several well publicized collections and uses of online personal information for unauthorized purposes, has focused the attention of consumers, privacy advocates, online service providers, Web sites, businesses, trade associations, courts, the Clinton Administration, and the Congress on the issue.

Federal Statutory Protections

In the United States there is no comprehensive legal protection for personal information. The Constitution protects the privacy of personal information in a limited number of ways, and extends only to the protection of the individual against government intrusions. Constitutional guarantees are not applicable unless "state action" has taken place. Many of the threats to the privacy of personal information addressed in this paper occur in the private sector, and are unlikely to meet the requirements of the "state action" doctrine. As a result, any limitations placed on the data processing activities of the private sector will be found not in the federal Constitution but in federal or state statutory law or common law.

A patchwork of federal laws exists to protect the privacy of certain types of personal information. There is no comprehensive federal privacy statute that protects personal information in both the public and private sectors. A federal statute exists to protect the privacy of personal information collected by the federal government.[10] The private sector's collection and disclosure of personal information has been addressed by Congress on a sector-by-sector basis. With the exception of the recently enacted Children's Online Privacy Protection Act of 1998, none of these laws specifically covers the collection of online personal information. Federal laws extend protection to credit,[11] electronic communications,[12] education,[13] bank account,[14] cable,[15] video,[16] motor vehicle,[17] health,[18] telecommunications subscriber,[19] and children's online information.[20]

The Clinton Administration's Approach to Internet Privacy

The federal government currently has limited authority over the collection and dissemination of personal data collected online. The Federal Trade Commission Act (the "FTC Act")[21] prohibits unfair and deceptive practices in and affecting commerce. The FTC Act authorizes the Commission to seek injunctive and other equitable relief, including redress, for violations of the Act, and provides a basis for government enforcement of certain fair information practices (e.g., failure to comply with stated information practices may constitute a deceptive practice or information practices may be inherently deceptive or unfair). However, as a general matter, the Commission lacks authority to require firms to adopt information practice policies.

The Federal Trade Commission has brought enforcement actions under § 5 of the Federal Trade Commission Act to address deceptive online information practices. In 1998, GeoCities, operator of one of the most popular sites on the World Wide Web, agreed to settle Commission charges that it had misrepresented the purposes for which it was collecting personal identifying information from children and adults through its online membership application form and registration forms for children's activities.[22] In its second Internet privacy case, the Commission announced a settlement with Liberty Financial Companies, Inc., operator of the Young Investor Web site. The Commission alleged, among other things, that the site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously. The consent agreement would require Liberty Financial to post a privacy policy on its children's sites and obtain verifiable consent before collecting personal identifying information from children.[23]

In June 1998, the Federal Trade Commission presented a report to Congress titled *Privacy Online*[24] based on its examination of the information practices of over 1400 commercial sites on the World Wide Web, and assessed private industry's efforts to implement self-regulatory programs to protect consumers' online privacy. This report included an analysis of 212 sites directed to children. The FTC identified five core principles of privacy protection which represent 'fair information practices': (1) consumers should be given *notice* of an entity's information practices before any personal information is collected from them; (2) consumers should be given *choice* as to how any personal information collected from them may be used; (3) individuals should be given the ability both to *access* data about him or herself and to contest that data's accuracy and completeness; (4) data collectors must take reasonable steps to ensure that data be *accurate and secure*; and (5) an effective *enforcement* mechanism must be in place to enforce the core principles of privacy protection. With these fair information practice principles and industry guidelines as background, the Commission conducted a survey of commercial sites on the World Wide Web.

Although the Commission has encouraged industry to address consumer concerns regarding online privacy through self-regulation, the Commission found that the vast majority of online businesses had yet to adopt even the most fundamental fair information practice of notice. Moreover, trade association guidelines submitted to the Commission did not reflect industry acceptance of the basic fair information practice principles, nor contain the enforcement mechanisms needed for an effective self-regulatory regime. In the specific area of children's online privacy, the Commission recommended that Congress develop legislation to control online collection.

The Federal Trade Commission issued a new report to Congress in July 1999 on *Self-Regulation and Online Privacy*[25] that assessed the progress made in the protection of consumers' online privacy since its June 1998 report. The Commission found that there has been notable progress in self-regulatory initiatives, and that online businesses are providing significantly more notice of their information practices. However, it found that the vast majority of the sites surveyed collect personal information from consumers online, and that the implementation of fair information practices is not widespread. In light of these results, the Commission concluded that further improvements are required to effectively protect consumers' online privacy. In the Commission's view, the emergence of online privacy seal programs (such as TRUSTe[26] and BBBOnLine[27]) is a promising development in self-regulation. These programs require their licensees to abide by codes of online information practices and to submit to compliance monitoring in order to display a privacy seal on their Web site. However, the Commission found that because only a handful of Web sites participated in online privacy seal programs, that it is too early to judge their effectiveness.

The Commission choose not to recommend legislation to address the protection of online privacy. Instead it developed an agenda to further address online privacy issues, and to assess progress in self-regulation. As part of its agenda, the Federal Trade Commission and the Department of Commerce recently held a Public Workshop on Online Profiling to assess the impact of "online profiling"—the practice of aggregating information about consumers' interests, gathered primarily by tracking their movements online, and using the profiles to create targeted advertising on Web sites.[28] Another part of its agenda includes conducting another online survey to reassess progress in Web sites' implementation of fair information practices.

The European Union Directive on the Protection of Personal Data

U.S. and EU officials have been engaged in informal dialogue concerning implementation of the EU Data Protection directive which focuses on the goals of enhancing data protection for European citizens while maintaining the free flow of personal information between Europe and the United States. The European Union Directive on the Protection of Personal Data became effective October 1998.[29] It comprises a general framework of data protection practices for the processing of personal data, which it defines as "any information relating to an identified or identifiable natural person," about European Union citizens. It will require each of the sixteen EU member states to enact laws governing the "processing of personal data." Significantly, the Directive obligates EU Member States to prohibit data transfers to non-European countries that do not have "adequate levels of protection" for personal data. Because the United States relies largely on a sectoral and self-regulatory, rather than legislative, approach to privacy protection, many U.S. organizations have been uncertain about the impact of the "adequacy" standard on personal data transfers from European Community countries.

In November 1998, the U.S. Department of Commerce adopted a "safe harbor" to permit U.S. companies that voluntarily adhere to the principles to continue transborder data transfers with EU Member states. The principles are not intended to govern or affect U.S. privacy regimes. The principles are designed to serve as guidance to U.S. organizations seeking to comply with the "adequacy" requirement of the directive, and would provide organizations within the safe harbor with a presumption of adequacy and data transfers from the European Community to them could continue. The International Safe Harbor Privacy Principles issued by the Department of Commerce are: notice, choice, onward transfer, security, data integrity, access, and enforcement.[30] The "enforcement" principle establishes mechanisms for ensuring compliance with the principles and includes independent recourse mechanisms, systems to verify the privacy practices of businesses, and obligations to remedy implementation problems arising from the principles.

The enforcement issue has been particularly problematic for the US-EU negotiators with focus on where enforcement actions would be brought to enforce the terms of the safe harbor (e.g., the U.S. or Europe), on who would be responsible for enforcement (either a U.S. government body such as the Federal Trade Commission or the courts, or a U.S. self-regulatory body such as BBB Online or Trust-E), and on under what circumstances could European authorities cut off data flows to the U.S. The U.S. has also expressed concern about the likelihood of actions, other than data blockages, being taken against U.S. companies including ordering erasure of data, ordering access to data, ordering rectification, and awarding damages. Another area of disagreement between the U.S. and the EU is over the effect of the Gramm-Leach-Bliley Act of 1999 (Pub. L. No. 106-102). The U.S. would like the European Commission to declare that the Act is "adequate protection" for the financial services sector, and also seeks a similar determination for the Fair Credit Reporting Act.

The Department of Commerce and the European Commission have initiated their respective governmental and public reviews of the "safe harbor" arrangement. On February 22, 2000, U.S. and EU officials announced that substantial progress in the negotiations has been made which could lead to resolution of the issue of the adequacy of the U.S. self-regulatory approach to data privacy.[31]

Congress' Response to Internet Privacy

Congress has also undertaken several initiatives aimed at protecting the privacy of online personal information. This year Congress established the Congressional Caucus on Privacy. Last year, Congress enacted the Gramm-Leach-Bliley Act of 1999,[32] financial services modernization legislation, that includes provisions to protect the privacy of personal information maintained by financial institutions. In addition, in the 106th Congress a number of online privacy bills have been introduced, and hearings have been held on online privacy. A chronological listing of congressional hearings on online privacy in the 106th Congress' follows (hearing testimony can be found at www.senate.gov and www.house.gov). In 1998, in response to the concerns over the privacy of children's online personal information, the 105th Congress passed the Children's Online Privacy Protection Act of 1998 (COPPA)[33] to prohibit unfair and deceptive acts and practices in connection with the collection and use of personally identifiable information from and about children on the Internet.

The Children's Online Privacy Protection Act of 1998

Section 1303 of the Act directs the FTC to adopt regulations prohibiting unfair and deceptive acts and practices in connection with the collection and use of personal information from and about children on the Internet. Section 1303(b) sets forth a series of privacy protections to prevent unfair and deceptive online information collection from or about children. The Act specifies that operators of Web sites directed to children or who knowingly collect personal information from children (1) provide parents notice of their information practices; (2) obtain prior parental consent for the collection, use and/or disclosure of personal information

from children (with certain limited exceptions for the collection of online information e.g., e-mail address); (3) provide a parent, upon request, with the ability to review personal information collected from his/her child; (4) provide a parent with the opportunity to prevent the further use of personal information that has already been collected, or the future collection of personal information from that child; (5) limit collection of personal information for a child's online participation in a game, prize offer, or other activity to information that is reasonably necessary for the activity; and (6) establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the personal information collected.

The Act authorizes the Commission to bring enforcement actions for violations of the final rule in the same manner as for other rules defining unfair and deceptive trade acts or practices under § 5 of the Federal Trade Commission Act. In addition, § 1305 of the Act authorizes state attorneys general to enforce compliance with the final rule by filing actions in federal court after serving prior written notice upon the Commission when feasible. The Commission issued a final rule fall 1999 to implement COPPA.

Congressional Hearings

In the 106th Congress, the following hearings have been held on online privacy:

Online Privacy hearing before the Senate Subcommittee on Communications, Committee on Commerce, Science, and Transportation, 106th Cong., July 27, 1999.

Electronic Commerce: Current Status of Privacy Protections for Online Consumers hearing before the House Subcommittee on Telecommunications, Trade and Consumer Protection, Committee on Commerce, 106th Cong., July 13, 1999.

Website Privacy Disclosure hearing before the House Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, 106th Cong., May 27, 1999.

Privacy in the Digital Age: Discussion of Issues Surrounding the Internet hearing before the Senate Judiciary Committee, 106th Cong., Apr. 21, 1999.

Conclusion

A host of questions are raised by the proliferation of online personal information. Does a business have a right to sell information about its customers without the customer's knowledge or consent? Should the collection of personal information by commercial Web sites be regulated? Is industry's self-regulatory approach to data privacy effective? What enforcement mechanisms exist for online users to remedy the unauthorized collection and use of personal information? Are the lack of adequate privacy protections for online personal information a deterrent to consumer participation in electronic commerce? Some advocate recognition of a right to "information privacy" for online transactions and personally identifiable information.[34] Others urge the construction of a market for personal information, to be viewed no differently than other commodities in the market.[35] The Congress, the executive branch, courts, businesses, privacy advocates, Web sites and Internet service providers, and trade associations continue to confront many of the issues associated with the privacy of online information in large part because the success of the Internet and electronic commerce depends upon the resolution of these issues.

Endnotes

1. *See* U.S. Govt. Information Infrastructure Task Force, *A Framework for Global Electronic Commerce* 10-12 (1997). Available: http://www.iitf.nist.gov/eleccomm/ecomm.htm.
2. For a list of Internet privacy legislation introduced in the 106th Congress *see*, Congressional Digest, *Internet Privacy: Protecting Personal Information Online* 43 (February 2000).
3. *See* generally Federal Trade Commission, *Privacy Online: A Report to Congress* (June 1998), http://www.ftc.gov/reports/privacy3/index.htm; *Self-Regulation and Online Privacy (July 1999),* http://www.ftc.gov/os/1999/9907/pt071399.htm; U.S. Govt. Information Infrastructure Task Force, *Options for Promoting Privacy on the National Information Infrastructure* (April 1997), http://www.iitf.nist.gov/ipc/privacy.htm; National Telecommunications and Information Administration, *Privacy and Self-Regulation in the Information Age* (June 1997), http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm.
4. *See, e.g.*, *McVeigh v. Cohen*, 983 F.Supp. 215 (D.D.C. 1998) (holding that the Electronic Communications Privacy Act forbids the federal government from seeking information about online communications system users unless: (1) it obtains a warrant issued under the Federal Rules of Criminal Procedure or state equivalent, or (2) it gives prior notice to the online subscriber and then issues a subpoena or receives a court order authorizing disclosure of that information).
5. *See* American Bankers Association, *Financial Privacy in America*, App. 3, Web Privacy Statements of Financial Institutions (1998), http://www.aba.com.
6. *See* American Civil Liberties Union, *Defend Your Data Campaign*, http://www.aclu.org/privacy. Center for Democracy and Technology, *Data Privacy*, http://www.cdt.org/privacy.
7. *See* Online Privacy Alliance, *Guidelines for Online Privacy Policies,* http://www.privacyalliance.org/resources/ppguidelines.html.
8. *See* Direct Marketing Association, *The DMA's Privacy Promise,* http://www.the-dma.org; Individual Reference Services Group, *Self-Regulatory Principles Governing the Dissemination and Use of Personal Data*, http://www.irsg.org/html/industry_principles_principles.htm.
9. *See* Vanderbilt University Owen Graduate School of Management, Commercialization of the World Wide Web: The Role of Cookies, http://www2000.ogsm.vanderbilt.edu/cb3/mgt565a/group5/paper.group5.paper2.htm.5. The *Privacy Act of 1974* places limitations on the collection, use, and dissemination of information about an individual maintained by federal agencies.
10. The Privacy Act regulates federal government agency record-keeping and disclosure practices. The Act allows most individuals to seek access to records about themselves, and requires that

personal information in agency files be accurate, complete, relevant, and timely. The subject of a record may challenge the accuracy of information. 5 U.S.C.A. § 552a (1999).

11. *The Fair Credit Reporting Act of 1970* ("FCRA") sets forth rights for individuals and responsibilities for consumer "credit reporting agencies" in connection with the preparation and dissemination of personal information in a consumer report. A consumer report contains identifying information, credit information, public record information, and information on inquiries. Under the FCRA consumer reporting agencies are prohibited from disclosing consumer reports to anyone who does not have a permissible purpose. 15 U.S.C.A. § 1681-81t (1999).
12. *The Electronic Communications Privacy Act of 1986* ("ECPA") outlaws electronic surveillance, possession of electronic surveillance equipment, and use of information secured through electronic surveillance. The ECPA regulates stored wire and electronic communications (such as voice mail or electronic mail), transactional records access, pen registers, and trap and trace devices. The ECPA prohibits unauthorized access to stored electronic communications and prohibits the 'provider of an electronic communication service' from disclosing the contents of a communication it stores or transmits. The ECPA also limits a provider's disclosure of transactional data to the government, but not to private parties. 18 U.S.C.A. §§ 2510-2522, 2701-2711(1999).
13. *The Family Educational Rights and Privacy Act of 1974* governs access to and disclosure of educational records to parents, students, and third parties. 20 U.S.C.A. § 1232g (1999).
14. *The Right to Financial Privacy Act of 1978* restricts the ability of the federal government to obtain bank records from financial institutions, and sets forth procedures for the federal government's access to bank customer records. 12 U.S.C.A. § 3401(1999).
15. *The Cable Communications Policy Act of 1984* limits the disclosure of cable television subscriber names, addresses, and utilization information for mail solicitation purposes. 47 U.S.C.A. § 551(1999).
16. *The Video Privacy Protection Act of 1988* regulates the treatment of personal information collected in connection with video sales and rentals. 18 U.S.C.A. § 2710(1999).
17. *Driver's Privacy Protection Act of 1994* regulates the use and disclosure of personal information from state motor vehicle records. The DPPA limits the ability of states, subject to certain exceptions, to sell personal information on drivers, motor vehicle owners and registrants, and motor vehicle identification card holders without consent. 18 U.S.C.A. § 2721(1999).
18. *The Health Insurance Portability and Accountability Act of 1996* (Pub. L. No. 104-191, codified at 42 U.S.C.A. 1320d note). The Administration Simplification provisions of the Act set a deadline of August 1999 for congressional action on privacy legislation for electronically transmitted health information, and requires the Secretary of Health and Human Services to issue privacy regulations by February 2000 in the absence of congressional action.
19. *Communications Act of 1934, as amended by the Telecommunications Act of 1996* limits the use and disclosure of customer proprietary network information (CPNI) by telecommunications service providers, and provides a right of access for individuals. 47 U.S.C.A. § 222 (1999).
20. *Children's Online Privacy Protection Act of 1998*, requires parental consent to collect a child's age or address, and requires sites collecting information from children to disclose how they plan to use the data. 15 U.S.C.A. § 6501 (1999).
21. 15 U.S.C.A. §§ 41 *et seq.* (1999).
22. *GeoCities*, Docket No. C-3849 (Feb. 12, 1999), http://www.ftc.gov/os/1999/9902/9823015d&o.htm.
23. *Liberty Financial*, Case No. 9823522, http://www.ftc.gov/os/1999/9905/lbtyord.htm.
24. Http://www.ftc.gov/reports/privacy3/index.htm.
25. Http://www.ftc.gov/os/1999/9907/pt071399.htm.
26. Http://www.truste.org/about/about_committee.html.
27. Http://www.bbbonline.com.
28. Http://www.ntia.doc.gov/ntiahome/privacy/workshop/frn-workshop.htm.
29. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data, Eur. O.J. L281/31 (Nov. 23, 1995).
30. Http://www.ita.doc.gov.
31. BNA Daily Report for Executives, *U.S., EC Indicate Progress Toward Resolving Data Privacy Dispute* (Feb. 23, 2000).
32. Pub. L. No. 106-102.
33. Title XIII, Omnibus Consolidated and Emergency Supplemental Appropriations Act, Pub. L. No. 105-277, 112 Stat. 2681, 15 U.S.C.A. § 6501 (Oct. 21, 1998).
34. *See* Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?"* 44 Fed. Comm. L.J. 195 (1992).
35. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 Stanford L. Rev. 1193, 1201 (1998).

Gina Marie Stevens is a legislative attorney with the Congressional Research Service, Library of Congress. She holds a J.D. from Albany Law School and is a member of the New York Bar.

Editor's Foreword

(Continued from page 5)

This issue, like the last, also benefited from the contributions of Patricia Salkin. Her inexhaustible supply of ideas and enthusiasm have been essential to the enterprise. And all three of us of Albany Law School's Editorial Board are indebted to the leadership of the Bar Association for its generous support and confidence, and to the Association's staff—Patricia Wood and Wendy Pike deserve special mention—whose assistance in putting this issue together was indispensable, as well as patient and understanding. Finally, we are grateful to our student editors for their dedicated service in taking care of all the nitty gritties of editing, sub-editing, cite checking, etc. Special thanks goes to Catherine Michelle Hedgeman, our outgoing Student Executive Editor.

Comments and suggestions are certainly welcome—indeed, encouraged. They may be communicated via the law school's Government Law Center, or to me directly via e-mail (vbonv@mail.als.edu), regular mail, or any other customary means.

Vincent Martin Bonventre

Internet Access and Employer Risk

By Michael S. Moran

During the past several years, New York State agencies and not-for-profit organizations have made a concerted effort to provide information and services over the Internet. As a consequence, governmental and private offices that rely on this information have found that they must provide Internet access to their employees. Frequently, the employer also opts to make Internet e-mail available to employees. Following deployment of these services, however, employers often find that some of the productivity gains realized through Internet and e-mail availability are eroded by wayward usage. Moreover, certain employee abuses of Internet or e-mail systems may expose the employer to liability under state and federal statutes, regulations, and an emerging body of "Cybertort" case law. To effectively address these issues employers must turn to both legal and technical remedies.

The Information Revolution

Visitors to CorCraft's Web site can browse through the online catalog and place a secure order. At the Office of General Services site guests may search the newest State phone directory (and while there perhaps take a peek at the parking wait list). Web users can track pending legislation on the Senate's Web site or find a recent high court decision at the State Court of Appeals site. Educators may browse the State Education Department's Internet publications for the latest information on the new Learning Standards. Tax forms and retirement forms may be downloaded from the Department of Taxation and the Comptroller's office respectively. And Internet users in Buffalo could have watched the Chief Judge's State of the Judiciary Address broadcast live in streaming video from Albany earlier this year. These examples illustrate the remarkable breadth and quality of information available from New York governmental sites over the Internet. In many cases the fast and easy accessibility of this indispensable information makes Internet access essential for governmental and not-for-profit offices.

An Attractive Nuisance?

The Internet invites "browsing" and an unsuspecting or unscrupulous user can wander far afield with a few errant clicks. One recent survey of over 1,200 corporate Internet users found that more than 90% confess to visiting non-work related sites on company time.[1] In another study based on electronic monitoring data, Georgia Tech found that approximately 25% of employee Internet time was spent on personal activities.[2] Indeed, employers who provide Internet access cite the drain in resources as a result of recreational use as their chief concern.[3]

Hostile Work Environment Liability

Employer liability for an employee's misuse of electronic communications may be premised on discrimination, defamation, harassment, software piracy, copyright infringement or hostile work environment grounds. Although there is significant case law development in each of these areas, the so-called hostile work environment decisions are of particular import, and demonstrate how an employer can open itself to liability through sheer inaction.

The hostile work environment claim is derived from title VII of Civil Rights Act of 1964.[4] Title VII makes it unlawful for an employer to discriminate against any individual with respect to the "compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin."[5] In a decision addressing allegations of a sexually discriminating workplace, the Supreme Court rejected an employer's contention that "compensation, terms, conditions, or privileges" of employment ought to be limited to economic or tangible discrimination and found that the language of title VII evinces a congressional intent "'to strike at the entire spectrum of disparate treatment of men and women.'"[6] Title VII hostile work environment actions have also been extended to harassment based on race,[7] religion,[8] and national origin.[9]

To prevail in a claim for hostile work environment, a plaintiff must prove that he or she (1) is a member of a protected class; (2) was subjected to harassment that interfered with the employee's work or created an intimidating, hostile or offensive work environment; and (3) that a specific basis exists for imputing the con-

duct that created the hostile environment to the employer.[10] The environment must be both subjectively and objectively offensive.[11] Whether such an environment exists is a question of law.[12]

Several recent New York decisions discuss issues pertinent to an employer's potential liability in hostile work environment actions predicated upon misuse of office Internet or e-mail systems. An isolated misuse of an employer's e-mail system is not sufficient to create a hostile work environment.[13] The Federal Court of Appeals for the Second Circuit has held that

> for racist comments, slurs, and jokes to constitute a hostile work environment, there must be more than a few isolated incidents of racial enmity, meaning that instead of sporadic racial slurs, there must be a steady barrage of opprobrious racial comments. Thus, whether racial slurs constitute a hostile work environment typically depends upon the quantity, frequency, and severity of those slurs.[14]

Even if a hostile work environment is established, the employee must also show the employer's complicity therein. A manager's actual participation in the dissemination of offensive e-mail is sufficient to vicariously implicate the agency or company.[15] In cases where the discriminatory conduct creating the hostile work environment is attributable to a co-worker rather than a supervisor the plaintiff must demonstrate that management either "provided no reasonable avenue for complaint or knew of the harassment but did nothing about it."[16] Actual knowledge of the offending conduct is not necessary; it is enough if the employer "reasonably should know about" the harassment but fails to take appropriate remedial action.[17]

Although the law is just emerging in this area, it is possible that the courts may place an affirmative duty on employers to be vigilant as to their employee's e-mail and Internet behavior.[18] Even if an employer is not required to conduct ongoing general surveillance of its communications systems, it seems likely that some kind of investigatory onus would be placed on an employer who is confronted with a complaint. Indeed, the Court of Appeals for the Second Circuit has recently held that "allegations of sexual harassment trigger federal law and an attendant duty imposed upon employers to take reasonable steps to correct harassing behavior, including, where appropriate, conducting an investigation."[19]

What Is an Employer to Do?

Given the opportunity for employee abuse of Internet or e-mail systems as well as the potential liability for misuse of these systems, many employers have looked to technology for assistance. Some organizations have implemented Internet filtering solutions in an attempt to prevent employees from accessing sites with pornographic, racist, sexist, violent or gambling content. Some filtering products also seek to prevent employees from accessing news groups or chat rooms where an inflammatory message originating from an agency's Internet domain or e-mail address can prove embarrassing or even libelous. Some filtering offerings will also block access to popular recreational sites on the Internet in an effort to keep users on task. Filtering software may be installed on individual workstations,[20] or on a centrally managed network server.[21]

Internet filtering is imperfect, however. Often periodic updating of a downloadable "block list" of forbidden Web sites is required, and while many of the most frequently visited sites are listed, the dynamic nature of the Internet and the sheer number of pornographic and other undesirable sites makes exhaustive list-based filtering impossible. In addition, software that bases filtering on an analysis of Web site content may overzealously prevent access to legitimate sites (typically sites that run afoul of a customizable word dictionary are blocked), or conversely be fooled by cagey Internet purveyors.

E-mail filtering is even more troublesome than Internet filtering. While a blocked Internet site may be an annoyance to the affected employee, intercepted e-mail may interfere with a firm's operations, particularly when legitimate e-mail is inadvertently blocked. Consequently, most e-mail monitoring products do not rely exclusively on programmatic logic rules or word lists in determining whether or not e-mail should be subject to filtering. Typically, the suspicious message is automatically copied and forwarded to a designated person who reviews the e-mail contents and then warns the sender or receiver if the message is inappropriate or violates established policies. Clearly, this level of human intervention entails considerable agency or corporate overhead.[22]

The limitations of Internet filtering technology have caused some employers to abandon the notion of actively blocking access and instead rely to a large extent on more passive Internet monitoring as a deterrent.

Employer Monitoring of Employee Internet and E-mail Usage

Most monitoring software is designed for use in network environments rather than with single PCs with Internet connections. Typically the monitoring software is installed on a dedicated, networked computer equipped with a so-called "promiscuous mode" net-

work card (most are). Some products also require that the monitoring computer be connected or contiguous to the Internet router that provides Internet access.

The monitoring computer maintains a database of all IP packet activity, including Web, news, FTP, chat, and e-mail use. The software does not examine the content of each e-mail message or Web site, instead it records information such as site URL or sender's e-mail address, time of access and duration of the visit for each computer on the network. Some offices choose to routinely monitor this information, regularly looking for frequently visited sites or URLs with suspicious addresses.

Other employers forego routine policing of activity records, choosing to inspect database records only in the event of a complaint or other evidence of systems misuse. In this way, the monitoring software provides a means by which an employer can possibly verify indicia of misconduct. Even this limited type of inspection policy is likely to satisfy an employer's title VII obligations under the current state of the law.[23]

Monitoring and Privacy Implications

From an employer's perspective, Internet and e-mail monitoring address a variety of concerns that accompany Internet access. Monitoring can reduce employee visits to non-work related sites and the attendant drain on productivity. Monitoring can also minimize an employer's potential liability for an employee's discriminatory use of the communications system by discouraging access to pornographic and other offensive sites. In addition, monitoring can provide an employer who is confronted with a claim of harassment, discrimination or hostile work environment with the tools to conduct a meaningful investigation as required by recent cases construing title VII.

Monitoring itself raises various ethical, organizational and legal issues. Much of the litigation in this area has involved invasion of privacy claims. The threshold issue is whether an employer has the right to monitor employee Internet and e-mail activity at all. The consensus appears to be that a certain level of monitoring is within an employer's rights. "Employees should know that equipment given to them for business purposes is not theirs and the company has a legitimate interest in making sure it's used for business purposes. Companies have a responsibility and every legal right to track what's done with their technology."[24] However, an employer does not enjoy carte blanche surveillance rights. To determine what limitations do exist for employers in this area requires reference to the Constitution as well as federal and state legislation and case law.

Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 (ECPA) proscribes unauthorized retrieval or interception of electronic communications. 18 USC § 2702(a)(1), addressing retrieval, states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." The act defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications,"[25] but does not define "public." Courts have held that this provision is aimed at e-mail service providers serving the "community at large" rather than corporate or agency e-mail systems.[26]

Even firms within the purview of the ECPA may find relief in some of the exceptions provided by the legislation. Thus, while 18 USC § 2511 forbids the intransit interception of electronic communications generally, it carves out two relevant exceptions. A provider of electronic communication services can lawfully intercept electronic communications "while engaged in any activity which is a necessary incident to the rendition of his service."[27] In addition, the provider may legally intercept a communication if the provider is a party thereto or if one of the parties to the communication has given consent to the interception.[28] The exceptions contained in § 2511 are important guideposts for employers and will be revisited in the discussion of constitutional law and common-law privacy rights.

Section 2511 also states that it is not an offense for an electronic communications service provider to "record the fact that a wire or electronic communication was initiated or completed" if this is done to protect the provider or a user from "fraudulent, unlawful or abusive use of such service."[29] The "record the fact" language appears to condone employer monitoring of communications traffic data generally but does not specifically authorize a content-based employer intrusion. This may be indicative of a legislative preference for monitoring over the more intrusive filtering.

Fourth Amendment

The Fourth Amendment to the United States Constitution prohibits unreasonable searches and seizures. As Fourth Amendment guarantees extend only to "state action,"[30] searches involving private sector employers and employees are generally not within the amendment's reach. However, "searches and seizures by government employers or supervisors of the private property of their employees * * * are subject to the restraints of the Fourth Amendment."[31]

Courts have held that a Fourth Amendment violation occurs when an employer violates an employee's "expectation of privacy that society is prepared to consider reasonable."[32] A search conducted within an employer's scope of business is considered to be reasonable. "The governmental interest justifying work-related intrusions by public employers is the efficient and proper operation of the workplace."[33] Such searches need not be based on probable cause, but there must reasonable grounds for "suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct."[34] The likelihood remains that certain intrusions into office communications may invoke Fourth Amendment protections. "Not everything that passes through the confines of the business address can be considered part of the workplace context."[35]

Importantly, an employer's policies and practices may influence whatever expectations of privacy an employee may have and thereby change the legal balance. In *Bohach v. City of Ren,* the Federal District Court held that an employer's confiscation of messages stored in an agency's pager message system was not actionable under the Fourth Amendment.[36] After finding that agency employees had been notified that their electronic communications were "logged on the network" and that specified messages had been prohibited, the court concluded that the employer's notifications resulted in a "diminished expectation of privacy."[37] Similarly, the United States Supreme Court in *O'Connor v. Ortega* took the absence of an inspection policy into account in finding a reasonable expectation of privacy in an employee's work space. The court noted, however, that "the absence of such a policy does not create an expectation of privacy where it would not otherwise exist."[38]

In *United States v. Simons*, an employee charged with possessing child pornography on a computer at a governmental agency alleged that review of Internet usage logs constituted an unlawful search under the Fourth Amendment.[39] Citing the agency's written policy notifying employees of the auditing of electronic activity (entitled "Permitted and Prohibited Official Use of the Internet"), the court stated that "[g]iven this policy, the Court does not find that Defendant, as an employee at [the agency], had a reasonable expectation of privacy with regard to any Internet use."[40]

Other Sources of Privacy Rights

Unlike 10 other states, New York does not provide a right to privacy in the State Constitution.[41] Nor do New York courts recognize a common-law invasion of privacy cause of action.[42] And while Civil Rights Law §§ 50 and 51 do afford certain privacy rights, these are limited to protection of a person's "name, portrait or picture" when used "for advertising purposes or for the purposes of trade."

State governmental agencies must comply with the "unreasonable search" proscriptions in New York Constitution article I, § 12. An illegal seizure under federal Constitution in federal courts is also an illegal seizure under federal and State Constitutions in state courts.[43] Given this "policy of uniformity between State and Federal courts,"[44] it is unlikely that state courts will depart from established federal court law,[45] although state courts may feel free to interpret the New York Constitution "when the Supreme Court has not addressed a specific issue or provided guidance for such an analysis in its 4th Amendment rulings."[46] The dearth of case law examining the interplay between constitutional search constraints and government employer monitoring of employee communications may provide state courts with an opportunity to participate in the charting of this legal course.

The Necessity of an Internet and E-mail Usage Policy

Many employers have sought to avoid potential Fourth Amendment and title VII pitfalls through the adoption of Internet and E-mail Usage Policies.[47] By promulgating and distributing policy statements disclosing communications systems monitoring and specifying approved and disapproved activities an employer can satisfy the notice exceptions in title VII[48] and circumscribe an employee's privacy expectations under the Fourth Amendment. Furthermore, the deterrent effects of Internet and e-mail monitoring are enhanced by a specific and well-publicized statement of approved and disapproved usage. Finally, any sense of unfairness that may accompany monitoring tends to dissipate upon publication of usage policies.[49]

E-mail and Internet Usage Policies should, at a minimum, contain the following provisions:

- Notice that e-mail may be read by office management or a designee.
- Notice that Internet, newsgroup, chat room and FTP usage may be monitored.
- Notice that (excessive) nonbusiness or any unprofessional use of electronic communications is prohibited.
- Notice that communications systems may not be used to harass or discriminate.
- Notice that any use of the office communications systems for an unlawful purpose will be reported to the appropriate authorities.
- Notice that any violation of usage policies may result in discipline including dismissal.

Naturally, acceptable usage policies must be tailored to the specific needs of each office. For example, in firms

where heightened security is a priority, policies might include stipulations prohibiting distribution of trade secrets or other confidential information. Offices should also be aware that certain jurisdictions may have more stringent requirements than others and these must be reflected in an employer's guidelines. Lastly, increased litigation in this area (harassment claims filed with the Federal Equal Employment Opportunity Commission rose 150% between 1990 and 1996), is certain to result in rapid evolution of workplace harassment and privacy law and employers should pay close attention to new developments.

The promulgation of a comprehensive Internet Usage Policy is only the first step in the satisfaction of an employer's obligations regarding employee Internet access. Indeed, such policies are wholly ineffective unless they are communicated to personnel. While actual consent is preferred, once an employee has been notified of systems monitoring and published usage policies, courts have indicated that his or her use of office systems may constitute implied consent to the monitoring and usage policies.[50] In practice, notice and consent published on paper or on screen will likely suffice so long as it is otherwise sufficient.

Employers must deploy the monitoring system fairly and under established procedures. All personnel should be subject to monitoring, including supervisory personnel. In addition, if any employer chooses to block or otherwise inspect the content of transmissions, it should be according to neutral criteria memorialized in written procedures. If an employer does not routinely inspect e-mail or Internet content, then any inspection should be based on reasonable cause (e.g., a complaint). Punishment for misuse of the system should also be based on articulated standards.[51]

Conclusion

In 1995 a subsidiary of Chevron Corporation settled a sexual harassment lawsuit for $2.2 million after a list entitled "25 Reasons Why Beer is Better Than Women" was distributed through its e-mail system.[52]

In October 1999, California Governor Gray Davis vetoed legislation that would have prohibited employer clandestine monitoring of employee e-mail and Internet usage. The bill would have required employees to sign or electronically verify (via click agreement) that they had read, understood and consented to the employer's monitoring policies. Under the bill, data collected by the employer would be made available for inspection and employees had the right to contest data and have it deleted if shown to be inaccurate. Senate Sponsor Debra Bowden argued that employers "don't have the right to spy on workers in changing rooms and restrooms, and they don't have the right to eavesdrop on employee telephone conversations. Why then should employers have the right to ransack their employees private electronic files without having to tell them it's company policy?" Defending his veto, Governor Gray cited increased employer liability as a concern, stating that existing avenues for employee redress, such as defamation or harassment causes of action, were sufficient.[53]

The modern workplace presents both unprecedented opportunities and perils for both employers and employees. Employers providing Internet and e-mail access may need to monitor system usage if only to provide a means to investigate in the event of a harassment or hostile work environment complaint. Along with Internet access, prudent employers also distribute policies containing notice of employee monitoring as well as clear statements of acceptable and unacceptable activities. The policy statement and authorization serve to provide the employer with the consent, actual or implied, necessary to certain Civil Rights Law defenses and concomitantly clarify the employee's expectation of privacy applicable to public employees under Fourth Amendment analysis. Once an employer undertakes to monitor Internet and e-mail usage it must do so in an even-handed fashion with a focus on business-related activities.

Many employers do not know where to start in preparing an Internet Usage Policy. The employer's legal counsel should, naturally, figure prominently in the preparation of this document, but even an experienced practitioner may not be familiar with the technology that is so critical to a complete understanding of the issues in this area. While some monitoring software manufacturers publish sample usage policies,[54] policy specialists are also available, of course, over the Internet.[55]

Endnotes

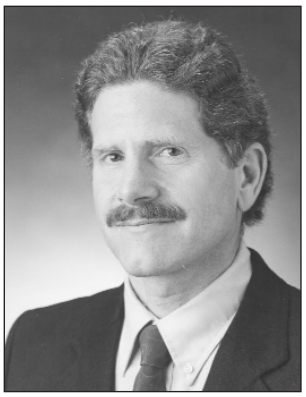
1. *See* Content Filters Don't Just Spy Risqué Surfing, PC Week, Nov. 29, 1999.
2. *See* Big Brother goes Web-watching, Employee Benefit News, Dec. 1, 1999.
3. *See* Newsbytes, (visited Oct. 3, 1997) <http://www.zdnet.com>.
4. *See* 42 U.S.C. §§ 2000e-17. It is uncertain whether New York courts will find "hostile work environment" protection in the State Human Rights Law (Executive Law §§ 290 *et seq.*). Although "[c]laims under the NYSHRL are similar to federal sexual harassment claims" New York courts may decline to follow the federal courts in establishing employer liability standards for workplace-based harassment under the State Human Rights Law. *Seepersad v. D.A.O.R. Sec.*, 1998 U.S. Dist. LEXIS 12465, 1998 WL 474205 (S.D.N.Y. 1998).
5. *See* 42 U.S.C. § 2000e-2(a)(1).
6. *Meritor Sav. Bank, FSB v. Vinson*, 477 U.S. 57 (1986).
7. *See Firefighters Inst. for Racial Equality v. City of St. Louis*, 549 F.2d 506, 514-15 (8th Cir.), cert. denied sub nom. *Banta v. United States*, 434 U.S. 819 (1977).
8. *See, e.g., Compston v. Borden, Inc.*, 424 F. Supp. 157 (S.D. Ohio 1976).

9. *See Cariddi v. Kansas City Chiefs Football Club*, 568 F.2d 87, 88 (8th Cir. 1977).
10. *See Briones v. Runyon*, 101 F.3d 287, 291-92 (2d Cir. 1996).
11. *See Faragher v. City of Boca Raton*, 524 U.S. 775 (1998).
12. *See Hardin v. Johnson & Son*, 167 F.3d 340, 345 (7th Cir. 1999); *Curtis v. DiMaio*, 46 F. Supp. 2d 206 (E.D.N.Y. 1999).
13. *See Curtis v. DiMaio*, 46 F. Supp. 2d 206 (E.D.N.Y. 1999); *Owens v. Morgan Stanley & Co.*, 1997 U.S. Dist. LEXIS 10351, 1997 WL 403454 (S.D.N.Y. 1997).
14. *Schwapp v. Town of Avon*, 118 F.3d 106, 110-11 (2d Cir. 1997); *see also*, *Schwenn v. Anheuser-Busch, Inc.*, 1998 U.S. Dist. LEXIS 5027, 1998 WL 166845 (N.D.N.Y. 1998).
15. *See Burlington Indus. v. Ellerth*, 524 U.S. 742 (1998); *Curtis v. Citibank, N.A.*, 1998 U.S. Dist. LEXIS 21, 1998 WL 3354, (S.D.N.Y. 1998); *see also*, *Curtis v. Citibank, N.A.*, 1999 U.S. Dist. LEXIS 11394, 1999 WL 544729 (S.D.N.Y. 1999).
16. *Van Zant v. KLM Royal Dutch Airlines*, 80 F.3d 708, 715 (1996); *Whidbee v. McDonald's Corp.*, 75 F. Supp. 2d 183 (S.D.N.Y. 1999).
17. *See Richardson v. New York State Dep't. of Correctional Serv.*, 180 F.3d 426 (2d Cir. 1999).
18. *See Burlington Indus.*, 524 U.S. at 765 (indicating an employer must use "reasonable care to prevent and correct promptly any sexually harassing behavior").
19. *Malik v. Carrier Corp.*, Nos. 98-7109, 98-7121 2000 U.S. App. LEXIS 960, *17, 2000 WL 85200, *6 (2d Cir. Jan. 26, 2000).
20. E.g., CyberPatrol <http://www.cyberpatrol.com>.
21. E.g., LittleBrother <http://www.littlebrother.com/index.html>; surfCONTROL SuperScout <http://www.surfcontrol.com/products/superscout/index.html>.
22. Prominent e-mail content security software manufacturers include Cameo from MicroData Group, Inc., MIMEsweeper from Content Technologies, Inc., ScanMail eManager from Trend Micro Inc., World/Secure Mail from Worldtalk Corp. and CommandView Message Inspector from Elron Software ("manage, filter and if necessary block company communications made through e-mail, news group and FTP sites").
23. *See* Malik, 2000 WL 85200 at *7, 2000 US App LEXIS 960 at *21 ("an employer's investigation of a sexual harassment complaint is not a gratuitous or optional undertaking; under federal law, an employer's failure to investigate may allow a jury to impose liability on the employer"); *see also*, *Torres v. Pisano*, 116 F.3d 625, 636 (2d Cir. 1997).
24. Eric Greenberg, American Management Association, quoted in Companies Move to Curb Web Surfing on the Job, Wash. Post, Dec. 20, 1999, at A01.
25. 18 U.S.C. § 2510(15).
26. *See Andersen Consulting v. UOP*, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998); *see also*, *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).
27. 18 U.S.C. § 2511(2)(a)(i).
28. *See* 18 U.S.C. § 2511(2)(d).
29. 18 U.S.C. § 2511 (2)(h)(ii).
30. *See Schowengerdt v. General Dynamics Corp.*, 823 F.2d 1328, 1332, n. 3 (9th Cir. 1987).
31. *O'Connor v. Ortega*, 480 U.S. 709, 715 (1987).
32. *United States v. Jacobsen*, 466 U.S. 109, 113 (1984).
33. *O'Connor*, 480 U.S. at 723.
34. *Id.* at 726.
35. *Id.* at 716.
36. 932 F. Supp. 1232 (D. Nev. 1996).
37. *Id.* at 1235; *see also*, *Adams v. City of Battle Creek*, 1999 U.S. Dist. LEXIS 6151 (W.D. Mich. 1999).
38. *O'Connor*, 480 U.S. at 719.
39. 29 F. Supp. 2d 324 (E.D. Va. 1998).
40. *Id.* at 327.
41. *See* Belanoff, Spelfogel & Bogue, E-mail: Property Rights vs. Privacy Rights in the Workplace, 45 Prac. Law 29 n. 8 (Dec. 1999).
42. *See Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538 (1902); *Brinkley v. Casablancas*, 80 A.D.2d 428 (1981).
43. *See People v. Gonzalez*, 39 N.Y.2d 122 (1976).
44. *People v. Johnson*, 66 N.Y.2d 398 (1985).
45. *But see*, *People v. Scott*, 79 N.Y.2d 474, 490 ("[W]e decline to adopt any rigid method of analysis which would, except in unusual circumstances, require us to interpret provisions of the State Constitution in 'Lockstep' with the Supreme Court's interpretations of similarly worded provisions of the Federal Constitution").
46. *Id.* at 407.
47. In a recent survey commissioned by Elron Software, 93% of large and mid-size organizations polled either had already implemented an Internet Usage Policy or planned to implement in the near future (1999 Corporate Internet Usage Survey, conducted by NFO Worldwide, Inc.). E-mail monitoring, which typically involves more intrusive content analysis, is significantly less common according to 1998 research (1998 survey of 1,000 corporations, conducted by American Management Association, finding 20.2 % of the organizations surveyed had implemented e-mail review practices).
48. *See Faragher*, 524 U.S. at 807 ("While proof that an employer had promulgated an antiharassment policy with complaint procedure is not necessary in every instance as a matter of law, the need for a stated policy suitable to the employment circumstances may appropriately be addressed in any case when litigating [a title VII] defense").
49. *See* PC World Online Survey (June 1997) (finding that 94.2 % of employees said their employer has the right to monitor how they use the Internet connection at work—provided they are informed first).
50. *See Griggs-Ryan v. Smith*, 904 F.2d 112, 117 (1st Cir. 1990) (explaining implied consent may be demonstrated by "language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private"); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1237 (D. Nev. 1996) (noting in dicta the court would have "implied consent in light of the plaintiffs' decision to send those messages via the computer").
51. *See Donovan v. Dewey*, 452 U.S. 594, 601 (1980) (indicating administrative searches must be conducted according to a "plan containing specific neutral criteria").
52. *See* Chevron Agrees to Pay $2.2 Million in Settlement, N.Y. Times, Feb. 22, 1995, at A16.
53. *See* Davis Vetoes Prohibition on Secret Monitoring of Worker Online, San Jose Mercury News, Dec. 12, 1999.
54. Elron Software publishes a sample Internet Usage Policy at <http://www.elronsoftware.com/enterprise/downloads.htm#manager>.
55. Jurifax, Inc., for example, provides customized Internet and e-mail use policies <http://www.jurifax.com/aindex.html>; e-mail usage templates are available through the Electronic Messaging Association <http://www.ema.org>.

Michael S. Moran, Esq., is the Chief Legal Editor, New York State Law Reporting Bureau.

The Impact of Technology on the Freedom of Information Law, a/k/a the "FOIL"

By Robert J. Freeman



When the New York Freedom of Information Law (FOIL) was enacted in 1974,[1] state and local government, like much of the rest of society, was tied to the typewriter and the photocopy machine. Many of us actually used carbon paper for our "cc's." Most searches for records were accomplished by pulling records from filing cabinets and reviewing them to determine the extent to which they must be disclosed.

Like the use of the term "FOIL," changes in technology have required us to reconsider a variety of words that now have new meanings. Foil is still used to wrap leftovers, but now "FOIL" can be a noun used to identify a statute or when requesting records ("I submitted a FOIL to obtain the plan submitted by the developer."); it has also become a verb ("I FOILed the record," or from the government agency's perspective, "We were FOILed."). "Encryption" was a word associated with wartime and spy novels. Now it's a part of communications that have become routine. A "password" used to be associated with a knock on the door. Now it's a tool that let's you in, or more importantly, keeps others out of your electronic information system. We've become concerned about viruses very different from those that kept our kids home from school. Going "online," engaging in "e-commerce," building "firewalls," "digital signatures" and developing an "Intranet" involve the use of terms redefined or that are completely new. For some of us, they have become part of our everyday vocabulary. And if they are not now, they will be soon.

Technology is changing the nature of the relationship between the government and the public it serves. At the heart of the relationship are the expectations of citizens in terms of the information they can acquire, the means by which they can acquire it, and the speed with which government can respond.

What Is a "Record"?

Soon after the enactment of FOIL, it became clear that the means by which we generate, exchange and maintain our records was changing, and by 1978, the original version of the FOIL was repealed and replaced with a modern statute that was drafted in a manner adaptable to changing information technology.[2] Since that time, FOIL has been based upon a presumption of access. Stated differently, all records of an agency are available, except to the extent that records or portions thereof fall within one or more grounds for denial appearing in § 87(2)(a) through (i). Most of the grounds for denial involve the ability of a government agency to withhold records to the extent that disclosure would result in harm to an individual with respect to an invasion of personal privacy, to a commercial entity when the release of records would cause injury to its competitive position, or to the government in terms of its capacity to carry out its duties effectively on behalf of taxpayers.

Perhaps as important as the statute's presumption of access is its scope. FOIL pertains to agency records, and § 86(4) defines the term "record" to include:

> any information kept, held, filed, produced, reproduced by, with or for an agency or the state legislature, in any physical form whatsoever including, but not limited to, reports, statements, examinations, memoranda, opinions, folders, files, books, manuals, pamphlets, forms, papers, designs, drawings, maps, photos, letters, microfilms, computer tapes or discs, rules, regulations or codes.

Based upon the language quoted above, if information is maintained by or for an agency in some physical form, it constitutes a "record" subject to rights of access conferred by the FOIL. The definition includes specific reference to computer tapes and discs, and it was held soon after the reenactment of the FOIL that "[i]nformation is increasingly being stored in computers and access to such data should not be restricted merely because it is not in printed form."[3]

"Creating" Records

FOIL pertains to existing records and states that an agency is not required to create a record in response to a request.[4] That was an easy concept to understand and implement in the era of paper. If an agency did not have a "list" of certain items or had no total of the cost of heating the town hall, it would not be required to prepare a list or review its twelve monthly heating bills and add the figures to arrive at a total. However, when information is maintained electronically, if the information sought is available under FOIL and may be retrieved by means of existing computer programs, an agency is required to disclose the information. In that kind of situation, the agency would merely be retriev-

ing data that it has the capacity to retrieve. Disclosure may be accomplished either by printing out the data on paper or perhaps by duplicating the data on another storage mechanism, such as a computer tape or disk. On the other hand, if information sought can be retrieved from a computer or other storage medium only by means of new programming or the alteration of existing programs, those steps would be the equivalent of creating a new record. As suggested earlier, since § 89(3) does not require an agency to create a record, an agency is not required to reprogram or develop new programs to retrieve information that would otherwise be available.[5]

Often information stored electronically can be extracted by means of a few keystrokes on a keyboard. While some have contended that those kinds of minimal steps involve programming or reprogramming, so narrow a construction would tend to defeat the purposes of the FOIL. Morever, extracting information and creating it clearly involve different functions.

If, for example, an applicant knows that an agency's database consists of 10 items or "fields," asks for items 1, 3 and 5, but the agency has never produced that combination of data, would it be "creating" a new record? The answer is dependent on the nature of the agency's existing computer programs; if the agency has the ability to retrieve or extract those items by means of its existing programs, it would not be creating a new record; it would merely be retrieving what it has the ability to retrieve in conjunction with its electronic filing system. An apt analogy may be to a filing cabinet in which files are stored alphabetically and an applicant seeks items "A," "L" and "X." Although the agency may never have retrieved that combination of files in the past, it has the ability to do so, because the request was made in a manner applicable to the agency's filing system. On the other hand, if the applicant makes a second request, this time for items 7, 8 and 9, but the agency has no method of retrieving or extracting those items except by means of new programming, i.e., changing the means by which it may retrieve or extract data, the act of reprogramming would be the equivalent of creating a new record, and an agency would not be required to do so. Going back to the filing cabinet in which the records are maintained alphabetically, the analogy would involve a request for the records filed, for example, between April and July of 1997. The agency knows that the items sought are kept within its files, but there may be no way of locating them, except by reviewing each individually. In that situation, the agency would not be required to alter its filing system, i.e., change it from alphabetical to chronological order, in an effort to accommodate the applicant. Based on the same logic, an agency would not be required to create a new program to extract that data that may be stored, but which cannot be retrieved or generated by means of its existing programs.

Notwithstanding an agency's inability to retrieve information sought unless it modifies its programs or reprograms, it may often be relatively simple to alter a program to retrieve the information sought. Moreover, it may be more cost efficient to engage in reprogramming than to delete portions of a printout by hand, for example, or to engage in a physical search of paper records. Redactions made manually and extensive searches are time consuming and labor intensive, but minor reprogramming may often be done quickly.

Format: Paper, Disk or Tape?

FOIL's statement of intent indicates that agencies are required to make records available "wherever and whenever feasible. What if the agency chooses to disclose a record by means of a computer printout, but the applicant has requested the record on a computer tape or disk? In *Brownstone Pub. Inc. v. New York City Dep't. of Bldgs.*,[6] the question involved an agency's obligation to transfer electronic information from one electronic storage medium to another when it had the technical capacity to do so and when the applicant was willing to pay the actual cost of the transfer. As stated by the Appellate Division:

> The files are maintained in a computer format that Brownstone can employ directly into its system, which can be reproduced on computer tapes at minimal cost in a few hours time—a cost Brownstone agreed to assume (see, POL [section] 87[1] [b] [iii]). The DOB, apparently intending to discourage this and similar requests, agreed to provide the information only in hard copy, i.e., printed out on over a million sheets of paper, at a cost of $10,000 for the paper alone, which would take five or six weeks to complete. Brownstone would then have to reconvert the data into computer-usable form at a cost of hundreds of thousands of dollars.
>
> Public Officers Law [section] 87(2) provides that, "Each agency shall . . . make available for public inspection and copying all records . . ." Section 86(4) includes in its definition of "record," computer tapes or discs. The policy underlying the FOIL is "to insure maximum public access to government records" (*Matter of Scott, Sardano & Pomerantz v. Records Access Officer*, 65 N.Y.2d 294, 296-297, 491 N.Y.S.2d 289, 480 N.E.2d 1071). Under the circumstances presented herein, it is clear that both the statute and its underlying policy require that the DOB comply with Brownstone's reasonable request to have the information, presently main-

tained in computer language, transferred onto computer tapes.[7]

In another decision, it was held that: "[a]n agency which maintains in a computer format information sought by a F.O.I.L. request may be compelled to comply with the request to transfer information to computer disks or tape."[8]

In short, assuming that the conversion of format can be accomplished, that the data sought is available under FOIL, and that the data can be transferred from the format in which it is maintained to a format in which it is requested, an agency would be obliged to do so. Under those conditions, production of the record would not involve creating a new record or reprogramming, but rather merely a transfer of information into a format usable to the applicant.

Fees

Section 87(1)(b)(iii) of FOIL stated until October 15, 1982, that an agency could charge up to twenty-five cents per photocopy or the actual cost of reproduction unless a different fee was prescribed by "law." Chapter 73 of the Laws of 1982 replaced the word "law" with the term "statute." As described in its annual report to the Governor and the Legislature by the Committee on Open Government (created by the enactment of FOIL in 1974 and reconstituted in the current statute[9]), which was submitted in December of 1981 and which recommended the amendment that is now law:

> The problem is that the term "law" may include regulations, local laws, or ordinances, for example. As such, state agencies by means of regulation or municipalities by means of local law may and in some instances have established fees in excess of twenty-five cents per photocopy, thereby resulting in constructive denials of access. To remove this problem, the word "law" should be replaced by "statute," thereby enabling an agency to charge more than twenty-five cents only in situations in which an act of the State Legislature, a statute, so specifies.[10]

Therefore, prior to October 15, 1982, a local law, an ordinance, or a regulation for instance, establishing a search fee or a fee in excess of twenty-five cents per photocopy or higher than the actual cost of reproduction was valid. However, under the amendment, only an act of the State Legislature, a statute, would permit the assessment of a fee higher than twenty-five cents per photocopy, a fee that exceeds the actual cost of reproducing records that cannot be photocopied, or any other fee, such as a fee for search. In addition, it has been confirmed judicially that fees inconsistent with the Freedom of Information Law may be validly charged only when the authority to do so is conferred by a statute.[11]

The specific language of FOIL and the regulations promulgated by the Committee[12] indicate that, absent statutory authority, an agency may charge fees only for the reproduction of records. Section 87(1)(b) of the Freedom of Information Law states:

> Each agency shall promulgate rules and regulations in conformance with this article . . . and pursuant to such general rules and regulations as may be promulgated by the committee on open government in conformity with the provisions of this article, pertaining to the availability of records and procedures to be followed, including, but not limited to . . .
>
> (iii) the fees for copies of records which shall not exceed twenty-five cents per photocopy not in excess of nine by fourteen inches, or the actual cost of reproducing any other record, except when a different fee is otherwise prescribed by statute."

The regulations promulgated by the Committee state in relevant part that:

> Except when a different fee is otherwise prescribed by statute:
>
> (a) There shall be no fee charged for the following:
>
> (1) inspection of records;
>
> (2) search for records; or
>
> (3) any certification pursuant to this Part.[13]

Based upon the foregoing, it is likely that a fee for reproducing electronic information would most often involve the cost of computer time, plus the cost of an information storage medium (i.e., a computer tape) to which data is transferred.

Although compliance with FOIL involves the use of public employees' time and perhaps other costs, the Court of Appeals has found that the Law is not intended to be given effect "on a cost-accounting basis," but rather that "Meeting the public's legitimate right of access to information concerning government is fulfillment of a governmental obligation, not the gift of, or waste of, public funds."[14]

E-mail Under FOIL

When I finished a draft of this article, I called Patricia Salkin at the Government Law Center and asked her if she wanted me to drop off a paper copy at her office, fax it to her, or to transmit it via e-mail. Among those choices, e-mail is clearly the easiest, the quickest and the cheapest. Once she received the article, she could

download it, format it in a way appropriate for the *Journal*, and edit it. In short, by using e-mail, we can do a great deal that we could not do nearly as efficiently in the recent past.

What had been yesterday's fantasy in terms of written communications has become today's reality. But along with the reality is a need to raise consciousness, a need to think of e-mail not merely as an instant means of leaving or responding to messages in a manner similar to phone calls and voice mail. Rather, we should think about e-mail for what it really is: an equivalent, in actuality and legally, to an old-fashioned letter or memo. In consideration of public rights of access, retention and disposal, and the functions and responsibilities of public employees, e-mail should be treated in most respects just like paper.

This is not to suggest that all e-mail communications must be disclosed. While FOIL is based on a presumption of access, it includes exceptions to rights of access. If e-mail is transmitted from one public employee to another, the most pertinent provision in analyzing rights of access would be § 87(2)(g), which deals with "inter-agency" and "intra-agency" materials. "Inter-agency" materials consist of written communications between or among employees of two or more agencies. "Intra-agency" materials are in-house communications. The letter from me at the Department of State to a school district official, for example, would constitute "inter-agency" material; the memo from the city clerk to the mayor would be "intra-agency" material. In both of those instances, § 87(2)(g) would bear upon rights of access, and it would apply whether the communications are transmitted on paper or via e-mail.

That provision permits an agency to withhold records that:

> are inter-agency or intra-agency materials which are not:
>
> i. statistical or factual tabulations or data;
>
> ii. instructions to staff that affect the public;
>
> iii. final agency policy or determinations; or
>
> iv. external audits, including but not limited to audits performed by the comptroller and the federal government. . . .[15]

It is noted that the language quoted above contains what in effect is a double negative. While inter-agency or intra-agency materials may be withheld, portions of such materials consisting of statistical or factual information, instructions to staff that affect the public, final agency policy or determinations or external audits must be made available, unless a different ground for denial could appropriately be asserted. Concurrently, those portions of inter-agency or intra-agency materials that are reflective of opinion, advice, recommendation and the like could in my view be withheld.

Several points should be emphasized in relation to the foregoing. First, that an internal communication does not represent or relate to a final agency determination does not remove it from the scope of rights of access. On the contrary, the content of the communication is the key to ascertaining how much can be withheld, or conversely, how much must be disclosed.[16] Second, "factual" information available under § 87(2)(g)(i) does not have to consist of numbers, charts or graphs; it might be a factual statement. "I looked out the window and the sky was blue" would be factual information that must be disclosed. And third, the exception does not apply to communications with persons or entities outside of government. An e-mail sent to or received by a member of the public or a private company, for example, would be neither inter-agency nor intra-agency material.

This communication from me at the Department of State, which is an "agency" as defined by FOIL, and the Government Law Center, which is part of Albany Law School and not a government agency, would not be covered by § 87(2)(g) and would have to be disclosed. Whether it is printed and delivered, sent by U.S. mail, faxed, or transmitted via e-mail, the result is the same: it is a "record" subject to FOIL that an agency would be required to disclose on request.

Retention and Disposal

Article 57 of the Arts and Cultural Affairs Law and the "Local Government Records Law," Article 57-A of that chapter, deal respectively with the management, custody, retention and disposal of records by state agencies and local governments.

With regard to the retention and disposal of records, § 57.05(11)(b) pertaining to state agencies and § 57.25 concerning local governments preclude state and local governments from destroying or disposing of records without following applicable procedures and until a minimum required period of retention has been reached. The provisions relating to the retention and disposal of records are carried out by a unit of the State Education Department, the State Archives and Records Administration (SARA). SARA has published *Managing Records in E-mail Systems*, which offers guidelines for developing policies and procedures for the effective management of records created and captured in e-mail systems.

Many of us have received e-mail messages, read them and then deleted them, for we have treated those communications like phone messages. For reasons described earlier, e-mail clearly constitutes a record for the purposes of FOIL, and it may have to be preserved under a SARA retention schedule. It is also important to

know that hitting the delete key does not mean that the record has been destroyed. Frequently the message that has been deleted can be found by hitting the "trash" key. In that situation, because the message still exists, it would be subject to FOIL or perhaps more importantly, to a subpoena or discovery in a lawsuit.

E-mail and the Open Meetings Law

There is nothing in the Open Meetings Law[17] that would preclude members of a public body, such as a city council or the board of a public authority, from conferring individually, by e-mail or telephone. However, a series of communications between individual members or telephone calls among the members which results in a collective decision, a meeting held by means of a telephone conference, or a vote taken by e-mail would be inconsistent with law. Voting and action by a public body may only occur at a meeting during which a quorum has physically convened.[18]

The Open Meetings Law is intended to provide the public with the right to *observe* the performance of public officials in their deliberations. That intent cannot be realized if members of a public body conduct public business as a body or vote by e-mail or phone.

A recent decision indicates that action taken by means of series of telephone calls violated the Open Meetings Law, and the same conclusion would likely be reached with respect to action taken through a series of e-mail communications. In *Cheevers v. Town of Union*,[19] the court stated that:

> There was no physical gathering, but four members of the five-member board discussed the issue in a series of telephone calls. As a result, a quorum of members of the Board were "present" and determined to [take an action]. The failure to actually meet in person or have a telephone conference in order to avoid a "meeting" circumvents the intent of the Open Meetings Law (see e.g., 1998 Advisory Opns Committee on Open Government 2877). This court finds that telephonic conferences among the individual members constituted a meeting in violation of the Open Meetings Law. . . .

If a majority of the members of a public body engage in "instant e-mail" or communicate in a chat room in which the communications are equivalent to a conversation, it is likely that a court would determine that communications of that nature would run afoul of the Open Meetings Law. In essence, the majority in that case would be conducting a meeting without the public's knowledge and without the ability of the public to "observe the performance of public officials" as required by the Open Meetings Law.[20]

E-mail can be a magical tool. An agency's well-designed and managed e-mail system can expedite business communications, reduce paperwork, increase productivity and diminish costs. Nevertheless, there should be an awareness of a variety of legal obligations, particularly those relating to FOIL, records management and even the Open Meetings Law.

The Need for Legislation

FOIL has clearly enhanced the ability of the public to know what the government is doing and to obtain information from or about government. Large amounts of information can be stored in electronic media and be made available quickly, efficiently and at low cost. Further, agencies are increasingly making information available via websites through which any person, anywhere can acquire data at virtually no cost, and without submitting a formal request under FOIL.

Despite the substantial improvements in the capacity of the public to use and agencies to comply with FOIL in a manner consistent with its intent, information technology can be used to make the law work better. The same technology has also created new pitfalls, danger in relation to the security of information maintained electronically, and new challenges for the State Legislature.

Guaranteeing Information Security

In 1984, FOIL was amended to enable agencies to withhold "computer access codes."[21] The idea was that disclosure of a code could result in unauthorized access to information stored in a computer. That was a first step toward protecting government records and information maintained electronically, but it is now clearly insufficient to guarantee against the legal disclosure of records that could be used not only to obtain information, but also to alter or even destroy it.

Not long ago, a description of an agency's security procedures concerning the protection of its records would not, if disclosed, compromise the ability to guard against unauthorized access. Even if written procedures were available, without the first key to unlock the door to the room in which the records were stored, and more importantly, without the second key needed to unlock the filing cabinet, records could be protected with reasonable certainty. In contrast, today's disclosure of an agency's security procedures could result in devastating attacks and incursions on its electronic information systems. The use of the key to unlock the door or filing cabinet, being physically present, is no longer necessary; an electronic attack can emanate from anywhere.

To ensure that the FOIL cannot be used to facilitate the unauthorized access to information stored electronically or to require the disclosure of security procedures that could damage an agency's information or information system, the Committee on Open Government has urged that the existing exception regarding computer

access codes be replaced with a new provision that permits agencies to withhold records or portions thereof that: ". . .would if disclosed facilitate unauthorized access to an agency's electronic information systems or clearly jeopardize or compromise information security."

Using Technology to Protect Privacy and Maximize Access

"One of the bedrock principles of electronic access is that format should not dictate the availability of information. In other words, if the information is available on paper, the fact that it is in electronic form should not be an obstacle to its availability."[22]

It is becoming increasingly critical to consider the design of information systems used by government in order to provide maximum access to records, while concurrently protecting against disclosure of deniable information, especially when disclosure would constitute an unwarranted invasion of personal privacy.[23] "The move to maintain and collect more government information in electronic form continues and it seems more likely that almost all records will at some time become electronic . . . [and] the real problems of balancing access and privacy will have to be faced and resolved in an electronic world."[24]

Through the design of information systems that provide appropriate disclosure coupled with the protection of personal privacy, often an agency need only delete certain fields from a database. Once the fields containing protected information are deleted, the database becomes fully public. Clearly that course of action, accomplished in consideration of access and privacy, is far preferable to a denial of access or the hours expended by agency employees making deletions with magic markers so that disclosure requirements can be met while recognizing the need to protect privacy.

In conjunction with the foregoing, the Committee on Open Government has recommended that a new § 89(9) be added to FOIL as follows:

> When records maintained electronically include items of information that would be available under this article, as well as items of information that may be withheld, an agency in designing its information retrieval methods, whenever practicable and reasonable, shall do so in a manner that permits the segregation and retrieval of available items in order to foster maximum public access.

Conclusion

It is clear that information technology has revolutionized the manner in which society, including government, creates, disseminates, stores and protects its information resources. In most respects, FOIL is adaptable to changing technology: it can and should be implemented in a manner that guarantees maximum public access to government records, while concurrently protecting against disclosures in accordance with exceptions to rights of access and a recognition of the need to assure security.

Endnotes

1. Originally N.Y. Pub. Off. Law, Article VI, §§ 85-89 (1974).
2. Ch. 933, L. 1977, Pub. Off. Law, Article VI, §§ 84-90 (1978).
3. *Babigian v. Evans*, 427 N.Y.S.2d 688, 691 (1980); *aff'd* 97 A.D.2d 992 (1983); *see also*, *Szikszay v. Buelow*, 436 N.Y.S.2d 558 (1981).
4. Pub. Off. Law, § 89(3) (1999).
5. *See Guerrier v. Hernandez-Cuebas*, 165 A.D.2d 218 (1991).
6. 166 A.D.2d 294 (1990).
7. *Id.* at 295.
8. *Samuel v. Mace*, (Sup. Ct., Monroe County, December 11, 1992); *aff'd* 190 A.D.2d 1067 (4th Dep't 1993).
9. Pub. Off. Law, § 89(1).
10. *See Annual Rep. to the Governor and Legislature by the Committee on Open Government* (December 1981).
11. *See Gandin, Schotsky & Rappaport v. Suffolk County*, 640 N.Y.S.2d 214, 226 A.D.2d 399 (1996); *Sheehan v. City of Syracuse*, 521 N.Y.S.2d 207 (1987).
12. 21 N.Y.C.R.R. Part 1401.
13. 21 N.Y.C.R.R. 1401.8.
14. *Doolan v. BOCES*, 48 N.Y.2d 341, 347 (1979).
15. Pub. Off. Law, § 87(2)(g).
16. *See Gould, Scott and DeFelice v. New York City Police Dep't*, 653 N.Y.S.2d 54, 89 N.Y.2d 267 (1996); *Xerox Corp. v. Town of Webster*, 65 N.Y.2d 131, 490 N.Y.S.2d 488 (1985); *Ingram v. Axelrod*, 90 A.D.2d 568 (1982).
17. Pub. Off. Law, Article VII, §§ 100-111.
18. Gen. Constr. Law, § 41 (1999).
19. Sup. Ct., Broome County, September 3, 1998.
20. *See* Open Mtgs. Law § 100 (1999).
21. Ch. 283, L. 1984.
22. Harry Hammitt, Government Technology (November 1997).
23. Pub. Off. Law, §§ 87(2)(b), 89(2), 96.
24. *See supra* note 20 and accompanying text.

Robert J. Freeman, Esq., is the Executive Director of the Committee on Open Government. Before becoming Executive Director of the Committee in 1976, Mr. Freeman had been its counsel. He received his law degree from the New York University and a B.S. in Foreign Service from Georgetown University in Washington, D.C.

DNA: Ending Crime as We Know It

By Peter Reinharz

All across America people are heralding the drop in the rates of violent crime. Large cities like New York have seen murder, rape and aggravated assault plummet over 60% in the last seven years. Even a slight increase in New York's homicide rate has not dampened spirits that violent crime can be consistently brought under control.

Beyond novel policing techniques are new technologies designed to aid law enforcement which have the potential to drive crime rates lower than they have been at any time in modern history. First on this list of scientific advances, is the genetic identification of criminals through the matching of DNA.[1]

DNA patterns provide unique genetic markings for every individual. Scientists can use these sequences to establish paternity, to link crime scene evidence to any perpetrator or to link evidence at crime scenes to establish the pattern of a serial offender. Using the latest technology developed for FBI standards, the DNA molecule is marked at 13 spots—called loci—and comparison is made between the suspect's DNA and the sample recovered at the crime scene. These 13 sites are considered "junk" sections of DNA since no inheritable characteristics are known to be associated with those portions of the molecule.[2] A match at all 13 sites renders the chances of two randomly selected people matching the DNA found at the crime scene greater than 1 in 1 trillion.[3]

It is this high degree of accuracy which makes DNA science so attractive to law enforcement officials. New York Courts have accepted the scientific reliability of DNA fingerprinting since 1994.[4] Newer cases have permitted the introduction of more modern methods of DNA evidence which allow proponents to quickly analyze DNA samples and provide results within 36 hours.[5] These new methods, Polymerase Chain Reaction (PCR) and Short Tandem Repeats (STR) can even allow degraded samples to be analyzed and typed.[6] The result of the PCR and STR analysis is a printed bar code which can provide scientists, courts and jurors with the ability to conclude whether a defendant is the "right person" or whether the case must be dismissed. DNA identification, has taken criminal jurisprudence to new levels of sophistication. DNA analysis allows courts to go beyond a determination of "guilty" or "not guilty," permitting inquiry into the realm of *innocence*.

Perhaps the most dramatic proof of DNA's effectiveness is not its ability to assure a conviction, but rather its capacity to exonerate those wrongfully convicted. Most notorious of these cases is that of Kevin Green an ex-marine who was charged in California with the attempted rape and murder of his pregnant wife. Green left his home with his wife asleep to get a hamburger. When he returned he found her bludgeoned and unconscious body barely alive. Detectives immediately focused on Green as a suspect and, upon testimony from his wife that she recalled the defendant with a blunt object in his hand, the State had their conviction. It was not until 16 years later that Green would be freed based upon a retest using DNA technology. The test results led police to another inmate, a serial rapist and murderer known as the Bedroom Basher, who subsequently confessed to the crime.

DNA use as a law enforcement tool will help change the way we measure public safety in the 21st century. In England the use of DNA has already had a tremendous effect upon the ability to solve crime. Unlike the U.S. where state and federal governments have been slow to start collecting and analyzing DNA from suspects, the English have already gathered more than 500,000 DNA samples from arrestees. They test these samples—taken at arrest by swiping the inside of an arrestee's cheek with a cotton "buccal" swab—and place the resulting codes in computers where they are matched against samples from crime scenes. For these efforts, the British, in the last 5 years, have linked over 70,000 suspects to crimes and are getting about another 500 matches per week.[7] Through the Forensic Science Service (FSS)[8] the English also test for DNA at unsolved crime scenes in the hopes that a subsequent arrestee will match the genetic profile of the unapprehended offender.

But in the U.S., the use of DNA as a forensic tool—despite its acceptance as admissible evidence in court—has not been as widespread. Unlike Britain's huge accomplishment in identifying tens of thousands of offenders via DNA technology, American law enforcement can only attribute about 1,000 solved crimes to DNA use. This low rate of success is proof positive that U.S. officials have failed to embrace some of the most

amazing technological feats that DNA has provided for English police and prosecutors.

Among the best demonstrations of DNA's power to catch violent criminals is the 1998 arrest of Charles "The Duck Robber" Peterson. Peterson was a suspect in a string of burglaries and two rapes in St. Petersburg, Florida when police asked him to provide a genetic sample for testing against evidence recovered at the crime scenes. When Peterson refused to provide the sample Florida police followed him as he drove around the gulf coast area on his motorcycle. When Peterson stopped at a traffic light he leaned over and spit into the street. The quick-thinking detective pulled up to the saliva in his unmarked car and took a paper towel to gather the evidence from the pavement. Based upon this unexpected expectoration, Peterson was matched by the DNA evidence to the crimes.

So with the success of DNA in England, and its obvious potential for law enforcement and exoneration of the innocent in America, why has DNA technology been so slow to become a regular part of criminal justice in the U.S.? The biggest objection to DNA technology has come from civil libertarians who see the technology as part of a brave new world where genetic coding sacrifices privacy and enables a new form of discrimination based upon our biological predisposition.

Leading the fight against the collection of genetic data is the American Civil Liberties Union. According to the ACLU, "the government and the private sector are in the process of carrying out the most frightening invasion of personal privacy in the nation's history."[9]

While calling the collection of DNA "the most frightening invasion" of personal security in American history is probably no more than eloquent hyperbole, there is sufficient justification for ensuring that protocols are established to guarantee that genetic information is not inappropriately distributed. In a short time scientists will have mapped the entire human genome which may enable researchers to determine whether people have predispositions for heart disease, colon cancer and other fatal ailments. While such information would clearly be helpful to those individuals so that appropriate prevention regimens are followed, the information in the hands of insurance companies could result in the denial of coverage. Further, a predisposition to particular diseases may cause employers or prospective employers to hire or fire someone who is genetically linked to a future chronic illness.

For these reasons it is important that government and private industry be held to strict standards regarding the retention of DNA samples and the distribution of genetic information. The rights of individuals can be protected if the legislatures carefully adopt laws—and localities adopt procedures—that will assure privacy and at the same time provide police with tools to apprehend more offenders.

Commissioner Howard Safir of the New York City Police Department has offered a plan which would provide maximum efficiency for law enforcement, but would also assure that genetic information would not be made available in such a way as to interfere with individual privacy. He suggests the following:

- All misdemeanor and felony arrestees should have their DNA sample taken via buccal swab.[10]
- State legislatures must fund the collection and analysis of all DNA samples and send the information into a national database for the tracking of offenders.
- The federal government should establish a database for the collection of DNA information from all arrestees under both federal and state jurisdiction.
- The United States should follow the lead of English law enforcement and establish an independent laboratory—like the FSS—for the testing of all DNA samples. The advantage of such a lab would be that it could serve both the prosecution and defense without any interest in test results or case outcomes.

Objections to these suggestions assert that taking DNA information from arrestees—rather than convicts—somehow disturbs the presumption of innocence and further erodes the privacy of the general public.[11] It is quite clear that the taking of DNA samples from convicts—at least from violent offenders or sex offenders – meets the requirements of most state courts. The recent decision from the Massachusetts Supreme Court in *Landry v. Attorney General* [12] found no Fourth Amendment violation in the taking of blood (for DNA typing) from convicted felons, and suggested that the crime control benefits eclipsed the privacy concerns of the prisoners. "[T]he high government interest in a particularly reliable form of identification outweighs the minimal intrusion of a pin prick."[13]

It is the reliability of DNA evidence that supports the need for its everyday use in law enforcement. Just like fingerprinting and photographing at arrest serves as a record of identification for police and prosecutors, so too should DNA be accepted as a refinement of these identification tools. It is true that DNA evidence can tell police far more about a person than a standard fingerprint, but such a benefit to law enforcement should hardly affect the Fourth Amendment question of whether the taking—i.e., the search and seizure—of the sample is *reasonable*.

Further, the privacy interests of a suspect should not be dependent upon the fact that one form of identification is less exact than another. The fact that fingerprints cannot tell us as much as DNA, in no way suggests that ink fingerprinting's shortcomings make it a less objectionable form of identification. Both systems are designed to identify a suspect and both allow police to isolate an offender from thousands of others using computer technology. So long as both systems remain solely available to law enforcement for identification purposes only, then the privacy concerns of DNA's critics are no different with respect to either regimen.

In fact, courts have recognized the similarity between the taking of standard fingerprints and the genetic coding of DNA from offenders.[14] "The State has an established and indisputable interest in preserving a permanent identification record of convicted persons for resolving past and future crimes and uses fingerprints, and now will use DNA identification, for these purposes."[15] Even more compelling is the opinion of the Fourth Circuit in *Jones v. Murray*[16]:

> [W]here the suspect is arrested upon probable cause, his identification becomes a matter of legitimate state interest and he can hardly claim privacy in it. We accept this proposition because the identification of suspects is relevant not only to solving the crime for which the suspect is arrested, but also for maintaining a permanent record to solve future and past crimes. . . . While we do not accept even this small level of intrusion for free persons without Fourth Amendment constraint, . . . the same protections do not hold true for those lawfully confined to the custody of the state. As with fingerprinting, therefore, we find that the Fourth Amendment does not require an additional finding of individualized suspicion before blood can be taken from incarcerated felons for the purpose of identifying them.[17]

Perhaps one of the ironies of the criticism of DNA identification is that those who seek to limit the use of genetic fingerprinting suggest that it is less intrusive than the standard fingerprinting and photographing of arrestees. But a buccal swab swipe of the cheek is much less cumbersome than having ten fingers and palms dipped into ink and then forcibly rolled onto paper by a detective. Similarly, it seems odd that DNA's antagonists would prefer traditional methods of arrest processing like photographing when such methods of identification do not come close to the one in a trillion odds offered by DNA technologies.[18]

Careful use of screening and storage protocols, will make it possible to meet most privacy concerns, while taking advantage of the benefits of the most advanced crime prevention techniques. As a way to allay the fears of those who worry about genetic profiling for commercial use, it would be best to destroy every sample (buccal swab or blood sample) after the material has been typed. The unauthorized distribution or reception of genetic information should be made a felony. Legislatures should also ensure the destruction of genetic identifiers (just like fingerprints and photographs) taken from acquitted persons, or those whose cases have been declined by prosecutors.

DNA technology affords America the chance to radically change the way it looks at and solves crime. It is time to take that chance and embrace DNA technology.

Endnotes

1. *See* Chembytes Series, *Crime Scene to Court* (visited Dec. 11, 1999) <http://www.chemsoc.org/ gateway/chembyte/forensic.htm> (explaining how DNA technology is used). DNA, short for deoxyribonucleic acid, is the molecule found in the nucleus of cells which contains the genetic code for every organism. The molecule contains a series of 4 proteins along two strands. These proteins, Adenine, Guanine, Thymine and Cytosine, bond to form base pairs linking both strands. The result is a double stranded DNA molecule of about 3 billion base pairs. The molecule is then twisted into a double helix shape—a shape that resembles a spiral ladder and has bonds between the base pairs as rungs. *See id*.
2. *See id*. (indicating this is important because using "junk DNA" sites permits police to identify offenders without having those sites reveal any other important genetic information about the person being tested).
3. *See* The California Dep't of Justice Crime Lab, San Francisco Chronicle, Oct. 19, 1999 at A1.
4. *See People v. George Wesley*, 83 N.Y.2d 417 (1994) (discussing the reliability of DNA identification within the scientific community).
5. *See People v. Qi Zhong Lin*, 699 N.Y.S.2d 294 (Sup. Ct. 1999) (accepting the PCR and STR typing methods as meeting sufficient reliability standards, permitting their admission into evidence in New York).
6. *See* Police Commissioner Howard Safir, Address to the International Association of Chiefs of Police on the Use of DNA Technology for Policing (Aug. 14, 1999) (explaining PCR and STR methods permit investigators to recover genetic material from the smallest amounts of blood, urine, semen or even from a sneeze at a crime scene, and indicating that DNA can now be recovered from the oil left behind by a suspect's fingerprint).
7. *See id*. (explaining the system used by the English to identify criminal suspects via DNA, and discussing the success of methods employed).
8. *See* Chembytes Series, *Crime Scene to Court* (visited Dec. 11, 1999) <http://www.chemsoc.org/ gateway/chembyte/forensic.htm> (identifying FSS as an independent laboratory system that contracts with local police throughout the country for all DNA analysis).
9. ACLU online Press Release April 14, 1999.
10. It is important to expand the group of persons tested beyond convicts to include all arrestees for misdemeanors and felonies.

Just as enforcement of quality of life offenses has revealed violent offenders out on warrants, so too will DNA typing from all arrestees allow for a greater chance to apprehend more violent offenders. The use of a computer database to keep this information will allow for more "cold hits" where the sample at a crime scene is matched to an unknown perpetrator whose genetic code is resident in the database. This is how Virginia investigators solved the 1994 rape and murder of Hope Denise Hall, whose killer was apprehended after police worked two years in vain to solve the crime via traditional police practices. Only a "cold hit" in the crime lab solved the case and the killer, a serial rapist named Shermaine Ali Johnson, is now on death row in Virginia.

11. Testimony of Barry Steinhardt, Associate Director, ACLU before the National Commission on the Future of DNA Evidence, March 1, 1999. "Arrest does not equal guilt and you shouldn't suffer the consequences of guilt until after you have been convicted." The testimony further states that the ACLU is opposed to the collection and storage of all DNA information. "Now I make no secret of the ACLU's opposition to DNA data banking, even for convicted felons."

    But see Bell v. Wolfish, 441 U.S. 520, 533 (1979) (stating that the presumption of innocence "has no application to a determination of the rights of a pretrial detainee during confinement before his trial has begun") Further, *Bell* makes clear that the use of correctional apparatus to pretrial detainees does not suggest the imposition of punishment. *See id*. at 534.

12. 429 Mass. 336 (1999).

13. *Id*. at 345 (citation omitted).

14. *See* Chembytes Series, *Crime Scene to Court* (visited Dec. 11, 1999) <http://www.chemsoc.org/ gateway/chembyte/forensic.htm> (noting that the inventor of DNA identification, Alec Jeffreys, called his process "DNA fingerprinting").

15. *Landry*, 429 Mass. at 347.

16. 962 F.2d 302 (4th Cir. 1992).

17. *Id*. at 306-07 (citations omitted).

18. The hazards of eyewitness and photograph identifications are well documented. *See People v. McDonald*, 37 Cal. 3d 351 (Sup. Ct., 1984). *See also* Frontline, *What Jennifer Saw: Summary of Cotton's Case*, (visited Feb. 8, 2000) <http://www.pbs.org/wgbh/pages/frontline/shows/dna/cotton/summary.html> (indicating the superiority of DNA technology over eyewitness and photo identification was featured on PBS' *Frontline* where Ronald Cotton, a convicted rapist in North Carolina, was finally freed by DNA evidence after having spent 10+ years in prison as a result of having been identified by witnesses via a photo and a lineup); Dr. Elizabeth Loftus & Katherine Ketcham, Witness for the Defense: The Accused, the Eyewitness, and the Expert who Puts Memory on Trial (1991).

Peter Reinharz, Esq., is the Chief of the Family Court Division, New York City Law Department.

The Creeping Expansion of DNA Data Banking

By Barry Steinhardt

I want to explain my fears about the creeping expansion of DNA data banking and the uses that this information will be put to. I want to explain what those fears are based on and to challenge those who advocate the use of DNA evidence in the criminal justice system to prove me wrong—to demonstrate that the lid can be firmly kept on Pandora's box.

Let me start with a point that I hope we can all agree on. Drawing a DNA sample is not the same as taking a fingerprint. Fingerprints are two-dimensional representations of the physical attributes of our fingertips. They are useful only as a form of identification. DNA profiling may be used for identification purposes, but the DNA itself represents far more than a fingerprint. Indeed, it trivializes DNA data banking to call it a genetic fingerprint; in Massachusetts, lawmakers have specifically rejected that term.[1]

I understand that the CODIS system[2] contains only a limited amount of genetic information compiled for identification purposes. But the amount of personal and private data contained in a DNA specimen makes its seizure extraordinary in both its nature and scope. The DNA samples that are being held by state and local governments can provide insights into the most personal family relationships and the most intimate workings of the human body, including the likelihood of the occurrence of over 4,000 types of genetic conditions and diseases. DNA may reveal private information such as legitimacy at birth and there are many who will claim that there are genetic markers for aggression, substance addiction, criminal tendencies and sexual orientation.

And because genetic information pertains not only to the individual whose DNA is sampled, but to everyone who shares in that person's blood line, potential threats to genetic privacy posed by their collection extend well beyond the millions of people whose samples are currently on file.

It is worth bearing in mind, too, that there is a long, unfortunate history of despicable behavior by governments toward people whose genetic composition has been considered "abnormal" under the prevailing societal standards of the day.

Genetic discrimination by the government is not merely an artifact of the distant past. During the 1970s, the Air Force refused to allow healthy individuals who carried one copy of the sickle-cell gene to engage in flight training, even though two copies of the gene are needed for symptoms of sickle-cell disease to develop. This restriction was based upon the then untested (and now known to be incorrect) belief that people with a single such gene could display symptoms of sickle-cell disease under low oxygen conditions, even though they would not actually have sickle-cell disease.[3]

Genetic discrimination by private industry is becoming increasingly commonplace as well. A 1997 survey conducted by the American Management Association found that six to ten percent of responding employers (well over 6,000 companies) used genetic testing for employment purposes.[4] The Council for Responsible Genetics, a nonprofit advocacy group based in Cambridge, Mass., has documented hundreds of cases in which healthy people have been denied insurance or a job based on genetic "predictions."

In short, there is a frightening potential for a brave new world where genetic information is routinely collected and its use results in abuse and discrimination.

Now, I am certainly aware that the primary purpose of forensic DNA databases like CODIS is identification and that the profiles are of 13 loci that currently provide no other information. However, I reject the term "junk DNA" because as the Human Genome Project and other studies continue those loci may well turn out to contain other useful genetic information.

The question then is why I am skeptical that we can hold the line and ward off the brave new world of genetic determinism?

In general, I am skeptical because of the long history of function creep. Of databases, which are created for one discrete purpose and, which despite the initial promises of the their creators, eventually take on new functions and purposes. In the 1930s promises were made that the Social Security numbers would only be used as an aid for the new retirement program, but over the past 60 years they have gradually become the universal identifier which their creators claimed they would not be.

Similarly, census records created for general statistical purposes were used during World War II to round up innocent Japanese Americans and to place them in interment camps.

We are already beginning to see that function creep in DNA databases. In a very short time, we have witnessed the ever-widening scope of the target groups from whom law enforcement collects DNA and rapid fire proposals to expand the target populations to new and ever greater numbers of persons.

In a less than a decade, we have gone from collecting DNA from convicted sex offenders—on the theory that they are likely to be recidivists and that they frequently leave biological evidence—to data banks of all violent offenders; to all persons convicted of a crime; to juvenile offenders in 29 states and now to proposals to DNA test all arrestees.

I am skeptical because too many state statutes allow evidence which has been purportedly collected only for identification purposes, to be used for a variety of other purposes. The Massachusetts law that the ACLU is challenging, for example, contains an open-ended authorization for any disclosure that is or may be required as a condition of federal funding and allows for the disclosure of information, including personally identifiable information for "advancing other humanitarian purposes."[5]

I am skeptical because there are proponents of these DNA database laws who continue to cling to notions of a genetic cause of crime. In 1996, the year before the Legislature's enactment of the law authorizing the Massachusetts DNA database, the Legislature commissioned a study to research the biological origins of crime that focused on the genetic causes.

That report specifically focused on genes as the basis for criminal behavior, stating: The report foresaw a future where "genetics begin . . . to play a role in the effort to evaluate the causes of crime," and even cited two articles regarding the debunked "XYY syndrome."[6]

I am skeptical too because too many holders of DNA data refuse to destroy or return that data even after the purported purpose has been satisfied.

The Department of Defense, for example, has three million biological samples it has collected from service personnel for the stated purpose of identifying remains or body parts of a soldier killed on duty. But it keeps those samples for information for *50 years*—long after the subjects have left the military. And the DOD refuses to promulgate regulations which assure that no third parties will have access to the records. Isn't it likely that once the genetic information is collected and banked, pressures will mount to use it for other purposes than the ones for which it was gathered, such as the identification of criminal suspects or medical research? In fact, on several occasions, the FBI has already requested access to this data for purposes of criminal investigations near military bases.

Similarly, many state laws do not require the destruction of a DNA record and/or sample after a conviction has been overturned or—in the case of Louisiana's incipient law—do not require that a person arrested for a crime of which he is not convicted automatically has his DNA records expunged.

The existence of private DNA databases in testing laboratories and government offices, that operate outside the relatively strict CODIS framework, also gives me reason for concern and skepticism.

I am also skeptical, when I hear from Professor Barry Scheck of discussions he has had with law enforcement officials who are considering DNA "dragnets" of neighborhoods or classes of people without informed consent. And I am particularly distressed by the trumpeting of the British model, with its expansive testing and where in one case all the young male inhabitants of a whole village were required to submit to blood or saliva tests.

And I am made more skeptical by sloppy practices that indicate that too few jurisdictions take seriously their obligations under the data bank regime to carefully preserve and test the samples that they do have. Only two state statutes, for example, mandate outside proficiency testing of DNA labs.

In short, the trend is away from limited-purpose forensic data banks. The purposes and target populations are growing and the trend is ominous.

Compounding this problem is that there are few laws, and certainly none at the federal level, which prohibit genetic discrimination by employers, insurers or medical care providers. More and more DNA is being collected, and with the advances in genetic research that make that DNA more and more valuable, instances of discrimination and misuse will grow as well.

Now let me turn to the specific question of DNA data collection from arrestees. Aside from supporting my suspicions that we will see an ever-widening circle of DNA surveillance, these proposals are fundamentally unfair, they violate the Constitution and even from a law enforcement perspective they are not practical—at least not at the moment.

Let's start with what I thought would be the obvious. Arrest does not equal guilt and you shouldn't suffer the consequences of guilt until after you have been convicted. The fact is that many arrests do not result in a conviction.

For example, a national survey of the adjudication outcomes for felony defendants in the 75 largest counties in the country revealed that in felony assault cases, half the charges were dismissed outright, and in 14 per-

cent of cases, the charges were reduced to a misdemeanor.

A study released by the California State Assembly's Commission on the Status of African American Males in the early 1990s revealed that 64 percent of the drug arrests of whites and 81 percent of Latinos were not sustainable, and that an astonishing 92 percent of the black men arrested by police on drug charges were subsequently released for lack of evidence or inadmissible evidence.

Indeed, there is a disturbing element of racial disparity that runs throughout our criminal justice system that can only be compounded by the creation of databases of persons arrested but not convicted of crimes.

Racial profiling and stereotyping is a reality of our criminal justice system. One study of police stops on a strip of interstate in Maryland gives some insight into the nature of the problem. Over several months in 1995, a survey found that 73 percent of the cars stopped and searched were driven by African-Americans, while they made up only 14 percent of the people driving along the interstate. While the arrests rates were about the same for whites and persons of color (approximately 28 percent), the disproportionate number of stops of minorities resulted in a disproportionate number of persons of color being arrested.

Now I make no secret of the ACLU's opposition to DNA data banking, even for convicted felons. We have argued and will continue to argue in cases like *Landry*[7] in Massachusetts that these are intrusive, unreasonable searches made without the individualized suspicion required by the Fourth Amendment and analogous provisions of state constitutions. But even if you accept the rulings that DNA data banking for convicted felons is permissible, either because a special need is present where persons have been convicted of crimes with high recidivism rates and the presence of biological evidence like sexual assaults, or that convicted felons have a diminished expectation of privacy, neither of those circumstances apply to persons who have simply been arrested.

To find otherwise is to equate arrest with guilt and to empower police officers, rather than judges and juries, with the power to force persons to provide the state with evidence that harbors many of their most intimate secrets and those of their blood relatives. Under the current circumstances of mistrust, that is an especially chilling notion for a New Yorker.

Take, for example, the "diminished expectations" argument on which most of the post-conviction DNA testing cases rest. Under this doctrine, the rights of persons who have been convicted of crimes become "diminished," only to the extent that those rights are "fundamentally inconsistent"[8] with the "needs and exigencies" of "the regime to which they have been lawfully committed."[9]

It cannot be argued that forcing arrestees to provide blood samples serves any legitimate security concern, even if they are in pre-trial detention. There are ample other means of confirming their identity. Nor by definition can DNA samples be used to insure compliance with any specified term of post-conviction supervised release. Put simply, these persons have not been convicted of any crime and may never be.

The only possible justification is investigatory and if law enforcement has reason to suspect an individual arrestee then it can and should seek a warrant.

If the special-exception doctrine makes any sense in the context of the post-convicted, it is based on the assumption that they have been found to have committed a crime where the recidivist rate is high and the presence of biological evidence is likely. How can you justify forced testing of a person arrested for jaywalking, or taking part in a political demonstration under that doctrine?

Now let me turn to the most practical of considerations—indeed the only consideration that gives me reason to hope that we will not move further down the path of DNA surveillance. As I read the literature, the single greatest obstacle to implementation of existing DNA data bank regimes is the large backlog of unprocessed samples. If I read the literature correctly, there is a backlog of 450,000 unprocessed samples and only 38,000 have been processed.[10]

There were 15 million arrests last year. From the law enforcement perspective does it really make sense to put the next dollars into collecting and processing samples for persons who have never been convicted of a crime; let alone a crime of the sort where DNA evidence is most likely to be probative. Wouldn't it make more sense to put scarce resources into processing the samples you already have and will generate in the future under the existing programs.

Let me say that I would love to be proved wrong. I would be more than happy to find that my fears are misplaced and that the civil liberties community is wrong about the likely future. If the advocates of DNA data banking can, in fact, restrict the uses of the data to forensic identification, if the data banks only cover persons convicted of a small number of crimes like sexual assault, if testing practices and data security are improved, all to the better. I won't mind being wrong. Pandora's box can be closed.

But the stakes are high and the risks are great. Every expansion of the data banks and every new use for the data increases those risks. The Commission has

an obligation not just to assist law enforcement, but to protect the privacy interests of all Americans.

We may not agree on what has come before, but I hope you will agree that if the line is not held here, it may never be held at all.

Endnotes

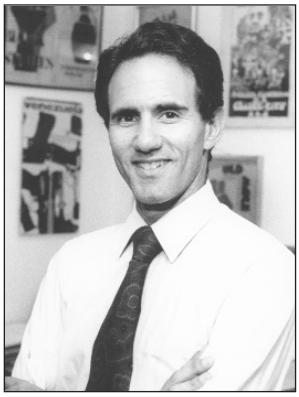
1. *Commonwealth v. Curnin*, 409 Mass. 218, 219 n. 2 (1991) (rejecting the use of the phrase "'DNA fingerprinting' because (1) it tends to trivialize the intricacies of the processes by which information for DNA comparisons is obtained (when compared to the process of fingerprinting) and (2) the word fingerprinting tends to suggest erroneously that DNA testing of the type involved in this case will identify conclusively, like real fingerprinting, the one person in the world who could have left the identifying evidence at the crime scene.").
2. Combined DNA Index System, "[a] collection of databases of DNA profiles obtained from evidence samples from unsolved crimes and from known individuals convicted of particular crimes. Contributions to this database are made through State crime laboratories and the data are maintained by the FBI." Jeremy Travis & Christopher Asplen, National Commission on the Future of DNA Evidence, NCJ Pub. No. 177626, Postconviction DNA Testing: Recommendations for Handling Requests 67 (1999).
3. E. Donald Shapiro & Michelle L. Weinberg, *DNA Data Banking: The Dangerous Erosion of Privacy*, 38 Clev. St. L. Rev. 455, 480 n. 132 (1990).
4. American Management Association, Workplace Testing & Monitoring (1997), *quoted in* Rosemary Orthmann, *Three-Fourths of Major Employers Conduct Medical and Drug Tests*, Employment Testing—Law & Policy Reporter (Jul. 1997).
5. Mass. Gen. Laws Ann. ch. 22E, § 10 (West 1999).
6. "Questions Concerning Biological Risk Factors for Criminal Behavior" (1996), *cited in* Brief of Amicus Curiae, Council for Responsible Genetics, *Landry v. Harshbarger* (No. SJC-07899), <http://www.aclu.org/court/landry/harshbarger_crg.html>.
7. *Landry v. Attorney General*, 429 Mass. 336 (1999) *cert. denied*, 68 U.S.L.W. 3153 (U.S.Mass. Jan 10, 2000) (No. 99-359) (holding that involuntary collection of DNA samples from persons subject to Massachusetts' DNA statute did not result in unreasonable search and seizure under the 4th Amendment and the State Constitution).
8. *Hudson v. Palmer*, 468 U.S. 517, 523 (1984).
9. *Wolff v. McDonnell*, 418 U.S. at 555-556 (1974).
10. National Commission on the Future of DNA Evidence, *CODIS Offender Database Backlog Reduction Discussion* (last modified Jan. 17, 2000) <http://www.ojp.usdoj.gov/nij/dnamtgtrans3/trans-k.html>.

Barry Steinhardt, Esq., is the Associate Director, American Civil Liberties Union.

This article is based on the author's testimony before the National Commission on the Future of DNA Evidence on Monday, March 1, 1999. Transcripts of his and other testimony before the Commission are available on line at http://www.ojp. usdoj.gov/nij/dna.

DNA Sampling on Arrest and the Fourth Amendment

By David H. Kaye



Every state and the federal government requires individuals convicted of certain felonies to provide DNA samples. These samples are analyzed for the presence of various individualizing features. The resulting, numerically coded "DNA profile" is stored in computers. By searching for matches between the recorded profiles and profiles derived from DNA in traces of blood, semen, or saliva associated with crimes, authorities have been able to identify hundreds of offenders. These early successes prompted proposals from law enforcement officials to take—and keep—DNA from individuals who are merely arrested. Although in most jurisdictions laboratories lack the capacity to handle the additional influx of samples that arrestee data banking would generate, it is only a matter of time until it will be feasible to analyze everyone's DNA.

But *should* we treat DNA like fingerprints and build searchable databases of identifying DNA information for some or all individuals who the police arrest for one reason or another? Or is the affront to personal privacy too grave a price to pay for the enhanced power to solve crimes and save lives? Does the constitution even permit such a police practice? Here, I offer an answer to the most powerful constitutional challenge that can be raised to sampling DNA on arrest—that it would be an unreasonable search or seizure under the Fourth Amendment.[1] I first argue that sampling and analyzing DNA should be considered a "search or seizure" that merits constitutional scrutiny. I then show that existing caselaw indicates that a carefully circumscribed database system that includes samples from arrestees could satisfy the Fourth Amendment.

DNA Databanking as a Search or Seizure

A threshold question in considering the constitutionality of DNA sampling under the Fourth Amendment is whether the acquisition of the sample is a search or seizure. If it is not, then the Fourth Amendment is no barrier. Making this determination requires an analysis of the method of collection used and the disposition of the sample. If sampling involves a physical intrusion into the body, the procedure is a search or seizure for Fourth Amendment purposes. If it is merely an inspection of material on the surface of the body, however, the collection of this material may not be, in and of itself, a search or seizure. Even so, subsequent analysis could reveal sensitive, personal information. For this reason, the Fourth Amendment is implicated when the government compels individuals to submit their DNA.

These conclusions follow from *Katz v. United States*[2] and its progeny. In *Katz*, the government acquired key evidence to convict the defendant of interstate gambling by attaching an electronic listening and recording device to the outside of a public telephone booth. The government argued that the interception was not a search because there was no physical trespass and the telephone booth was in a public place. The Supreme Court held that neither entry onto private property nor inspection of tangible items is an essential feature of a search, for "the Fourth Amendment protects people, not places."[3] It protected the defendant, the Court explained, because "a person in a telephone booth . . . who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[4] Because the federal agents had no warrant authorizing the interception, the majority held that the search violated the Fourth Amendment. In perhaps the most famous passage to emanate from the Justices in *Katz*, however, Justice Harlan wrote in his concurring opinion that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[5] Under *Katz*, the crucial threshold question for DNA sampling is whether society should recognize the expectation that the sample is not "up for grabs" by the government as reasonable.

Public Exposure and Knowledge

Public exposure of a bodily characteristic is highly significant in determining whether forcing the individual to reveal that characteristic to the government is a Fourth Amendment search. In *Katz*, the Court observed that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . ."[6] In *United States v. Dionisio*,[7] a grand jury subpoenaed twenty people to read the transcript of a tape recorded conversation aloud so that agents could record their voices and com-

pare them to those in the original conversation. Dionisio refused to cooperate and was held in contempt. The Supreme Court rejected his claim of Fourth Amendment protection. Explaining that "[t]he physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public,"[8] the Court held that neither the subpoena nor the recording process constituted a search or seizure.

The exposed-to-the-public principle, however, is ambiguous. *Dionisio* involved features that are casually and constantly observed in public. But what about features that are less widely known or not known at all by casual observers? Courts have extended the notion of "exposed to the public" well beyond the range of that which is constantly exposed and easily observed. Some courts, for example, have held that shining an ultraviolet lamp on an arrestee's skin to expose chemicals transferred from stolen money is not a search because the fluorescent material "'may be compared to a physical characteristic, such as a fingerprint or one's voice, which is constantly exposed to the public.'"[9]

Likewise, it might be argued that DNA is constantly exposed to the public. People shed hairs, cough or sneeze, expectorate, and even leave fingerprints that can contain cells. At best, however, the fact of such exposure is a relevant consideration in deciding whether the Fourth Amendment applies. *Dionisio* and cases extending it involve no intrusion into or touching of private areas of the body and no discovery of information about the individual beyond the identifying characteristics. Accordingly, even if the dubious position is taken that DNA is constantly exposed to the public in a meaningful way, whether these additional factors create a reasonable expectation of privacy must be considered.

Invasion of the Body and the Nature of the Information

Removing blood from the circulatory system invades bodily integrity, and as such, constitutes a search.[10] However, DNA can be obtained less invasively. Swabbing the inside of the cheek can provide cells for DNA analysis, but that, too, exceeds an inspection of the surface of the body presented to the public at large. Consequently, buccal swabbing is likely to trigger Fourth Amendment protection.[11] Saliva sampling presents a closer case because there is no entry into a body cavity.[12] Collecting DNA from exfoliating epidermal cells would be even less invasive than saliva sampling. These cells are on the outside of the body, where they are "visible" to the world in much the same sense as fingerprints. If an adequate number could be obtained by a procedure that is no more disturbing than fingerprinting, then both the site from which they are taken and the method of collection would suggest that this form of DNA sampling is not a search.

There is, however, a further consideration—the nature of the information that can be derived from the bodily material. If the DNA were obtained in a noninvasive manner and if only information related to identification could be obtained from it, the analogy to fingerprinting would be complete. Suppose that police were equipped with miniaturized DNA chips that could probe only noncoding loci[13] and that would automatically destroy the DNA once it has been analyzed and the profile recorded. This system might not rise to the level of a search. As currently practiced, however, DNA sampling should be considered a search and must be "reasonable" within the meaning of the Fourth Amendment.

Categorizing versus Balancing

The reasonableness of a search can depend on many things: the presence of a warrant, or, in the absence of a warrant, the feasibility or value of securing one; the extent and nature of the invasion of privacy; the purpose of the search; and the likelihood that it will achieve its goal. In theory, courts could inquire into the totality of the circumstances in each case, but in practice the courts usually apply categorical rules. Applying these rules to collecting and storing DNA information of arrestees, however, is neither simple nor free from doubt, and the constitutional analysis must attend to the following possible objections to DNA databanking: (a) there is no warrant and no probable cause (let alone reasonable suspicion) that the search will produce evidence of the offense for which the arrest is made; and (b) the sampling infringes bodily integrity and informational privacy. In several other situations where these objections have been raised, the Supreme Court has held that the government could undertake searches or seizures without a warrant and without individualized suspicion. If DNA databanking falls into one of the categories that these cases have established, it satisfies the Fourth Amendment. If it does not, the question of whether a new exception should be created arises—an inquiry that requires balancing the seriousness of the invasion of privacy against the governmental interests in the search.

The Identification Exception

The courts have long recognized the importance of accurately identifying individuals who are arrested. Although the Supreme Court has yet to bestow its formal blessing on routine fingerprinting or other identification procedures on arrest, it has intimated that inquiries that merely identify arrestees are valid,[14] and today most courts take the propriety of fingerprinting arrestees for granted. The procedure is a kind of inven-

tory search, providing an unequivocal record of just who has been arrested, that is considered appropriate when the state takes an individual into custody.[15]

Of course, recording biometric data that help establish the identity of those charged with crimes serves another function. Once the data have been justifiably obtained as part of the "inventory" of the arrested individual, they can be used to solve crimes unrelated to the one for which the arrest was made, on the ground that the further use does not amount to an independent invasion of privacy. For example, "mug shots" can be shown to a victim of a robbery in the hope that the victim will be able to identify the perpetrator or to exclude innocent subjects.[16] However, this investigatory use of biometric data is not what underlies the identification exception. The normal "identification exception" might be better denominated a "true identity" exception, since it merely relates to the government's need to know precisely who it has arrested.

Although the identity exception seems well established, whether DNA typing can be subsumed within it is less clear. On the one hand, fingerprints already provide an unequivocal, and in some respects, a better record of personal identity than forensic DNA typing. Monozygotic twins can be distinguished by their fingerprints, but not by their DNA. In addition, with current technology, fingerprints can be obtained more easily and more cheaply than DNA profiles. On the other hand, fingerprint patterns cannot be converted into numerical data that can be searched as efficiently as DNA data, and it is not obvious why the state should be confined to only one biometric identifier. An arrestee might be carrying false identification, and searching a database of DNA profiles of individuals with outstanding warrants might reveal that the arrestee is a fugitive. Thus, the narrow, "true identity" exception might well pertain to DNA genotyping as much as it does to fingerprinting.

The "Special Needs" Exception

A relatively recent and somewhat amorphous category of searches that do not require a warrant or individualized suspicion goes under the rubric of "special needs." These cases involve searches undertaken for some purpose other than the interception of contraband or the discovery of evidence of crime. As indicated in *National Treasury Employees Union v. Von Raab*,[17] "where a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context."[18] In these cases, the Court has considered the importance of the government's interest, the practicality and value of securing a warrant and requiring individual suspicion, and the gravity of the privacy invasion.[19] It has upheld warrantless, suspicionless searches of many types: administrative inspections in "closely regulated" businesses;[20] stops for questioning or observation at a fixed Border Patrol checkpoint[21] or at a sobriety checkpoint;[22] routine or random blood testing and urinalysis of certain employees[23] and student athletes[24] (but not candidates for public office);[25] inspections and seizures for the purpose of inventorying and preserving an arrestee's possessions;[26] random "shakedown" searches of prison cells;[27] and even visual anal or vaginal examinations of pretrial detainees.[28]

In determining whether DNA databanking is subject to the "special needs" analysis, the pivotal question is whether the *raison d'etre* of the system is unrelated to probable cause for believing that the target of the search is guilty of a particular crime. Because this is true of DNA databanking for identification, it is likely that courts will apply the balancing test used in the special needs cases to this new practice.

The "Special Needs" Balancing

On one side of the ledger, the physical intrusion is minimal, especially if the surface of the skin is not penetrated. Certainly, it is far less offensive than the body cavity searches of arrestees upheld in *Bell v. Wolfish*.[29] Furthermore, if there is adequate assurance that profiling of only "vacuous" loci can take place, no additional privacy interests are implicated. Finally, there is no unjustified detention of the person or entry into the home or other property. In sum, if the collection and storage of the genetic information is properly structured, the effect on the security of "persons, houses, papers, and effects" is quite limited.

To be balanced against the individual interest in the security of the person, are the government's interests. In addition to the administrative reasons to record biometric data that show a person's true identity discussed in connection with the identification exception, DNA sampling on arrest can help reduce serious crime in two ways. First, if a database of trace evidence DNA profiles from unsolved crimes were in place, a new arrestee's profile could be compared to those in the unsolved crimes database. A "hit" could result in continued pretrial detention, prosecution, and conviction for the unsolved crime. Second, even if no unsolved crimes database exists, the arrestee's profile could be included in a database of DNA profiles from arrestees. DNA from an unsolved case could be compared to all the potential offender profiles. A "hit" in the arrestee database could help solve the new case.

These government interests should not be exaggerated. Many people who have been arrested already

have convictions, and already should be in a convicted-offender database. Arrestee databanking offers no new information about them. Of the remaining arrestees who have no previous convictions, many will be convicted of the crime for which they were arrested. Their profiles soon would be in the convicted-offender database anyway. Consequently, the total impact of taking DNA from arrestees could be small.[30]

But even a small advance in law enforcement might be enough to justify nonintrusive DNA databanking confined to innocuous, biometrically identifying information on the individual. If reliable data were to demonstrate that individuals arrested for various offenses tend to commit other offenses for which DNA evidence frequently is available, then the argument for allowing DNA sampling on arrest as a "special need" probably would prevail. Which way the balance tips is a close question, but one that probably would be resolved in favor of a minimally invasive, highly secure system for DNA databanking even at the point of arrest.

Endnotes

1. For a more complete discussion of this issue, along with other possible constitutional challenges to arrestee databanking, see D.H. Kaye, DNA Sampling on Arrest: An Interim Report to the Legal Issues Working Group of the National Commission on the Future of DNA Evidence (2000). That report, and hence the condensed version of it provided here, benefited from comments from Paul Giannelli, Fran Gilligan, Edward Imwinkelried, Ralph Spritzer, and members of the Working Group.
2. 389 U.S. 347 (1967).
3. *Id*. at 351.
4. *Id*. at 352.
5. *Id*. at 361 (Harlan, J., concurring).
6. *Id*. at 351.
7. 410 U.S. 1 (1973).
8. *Id*. at 14.
9. *State v. Holzapfel*, 748 P.2d 953 (Mont. 1988) (quoting *Commonwealth v. DeWitt*, 314 A.2d 27, 30-31 (Pa. Super. Ct. 1973)).
10. *See Schmerber v. California*, 384 U.S. 757 (1966).
11. *Cf. Cupp v. Murphy*, 412 U.S. 291, 295 (1973) (reasoning that the taking of fingernail scrapings "went beyond mere 'physical characteristics . . . constantly exposed to the public' . . . and constituted the type of 'severe, though brief, intrusion upon cherished personal security' that is subject to constitutional scrutiny").
12. *See, e.g., United States v. Nicolosi*, 885 F. Supp. 50 (E.D.N.Y. 1995); *State v. Reeves*, 671 P.2d 553 (Kan. 1983) (indicating most lower courts have held that compelling a person to produce a saliva sample is a search); *cf. Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989) (treating breath sampling of alveolar air and urine sampling as searches).
13. A noncoding locus is a location within the genome where the DNA does not code for proteins. Most of the loci used in forensic work are of the sort. The point is not so much that the loci are noncoding as it is that they do not reveal any socially significant information about the individual. *See* D.H. Kaye, *Bioethics, Bench, and Bar: Selected Arguments in* Landry v. Attorney General, 40 Jurimetrics J. __ (2000) (forthcoming).
14. *See Illinois v. LaFayette*, 462 U.S. 640, 646 (1983) (plurality opinion offering the fact that "inspection of an arrestee's personal property may assist the police in ascertaining or verifying his identity" as one ground for allowing a warrantless, inventory search of the shoulder bag of an incarcerated arrestee).
15. For cases approving of inventory searches of possessions or automobiles following an arrest, *see, e.g., Illinois v. LaFayette*, 462 U.S. 640 (1983); *South Dakota v. Opperman*, 428 U.S. 364 (1976).
16. Acquiring picture of lawfully detained individuals also is permissible under the theory that ordinary photography is not a search or seizure. *Cf. United States v. Dionisio*, 410 U.S. 1 (1973) (voice exemplar); *United States v. Mara*, 410 U.S. 19 (1973) (handwriting exemplar).
17. 489 U.S. 656 (1989).
18. *Id*. at 665-66 (citations omitted).
19. Whether the Court has given proper weight to these factors and correctly applied them in each case is doubtful. *See, e.g., New York v. Burger*, 482 U.S. 691, 718 (1987) (dissenting opinion).
20. *New York v. Burger*, 482 U.S. 691 (1987) (warrantless search by police of automobile parts junkyard to find evidence of stolen cars under a state statute regulating automobile dismantlers); *Donovan v. Dewey*, 452 U.S. 594, 598-599 (1981) (warrantless inspection of stone quarry pursuant to the Federal Mine Safety and Health Act of 1977); *United States v. Biswell*, 406 U.S. 311 (1972) (warrantless inspection of the premises of a pawnshop operator who was federally licensed to sell sporting weapons).
21. *United States v. Martinez-Fuerte*, 428 U.S. 543, 545-50, 566-67 (1976).
22. *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 447, 455 (1990).
23. *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989); *Skinner v. Railway Labor Executives' Ass'n*, 489 U.S. 602 (1989).
24. *Veronia Sch. Dist. 47J v. Acton*, 515 U.S. 646 (1995).
25. *Chandler v. Miller*, 520 U.S. 305 (1997) (striking down a Georgia statute that demanded that every candidate for any of fourteen state offices present a certificate from a state-approved laboratory reporting that the candidate passed a urinalysis drug test).
26. *Illinois v. LaFayette*, 462 U.S. 640, 644 (1983); *United States v. Edwards*, 415 U.S. 800, 804 (1974).
27. *Hudson v. Palmer*, 468 U.S. 517 (1984).
28. *Bell v. Wolfish*, 441 U.S. 520 (1979); *cf. Griffin v. Wisconsin*, 483 U.S. 868 (1987) (warrantless search of probationer's home was valid because special needs of the probation system made a warrant requirement impracticable and justified replacement of standard of probable cause by "reasonable grounds").
29. 441 U.S. 520 (1979).
30. However, knowing one's DNA is on file could raise the perceived probability of apprehension and thereby deter some offenses.

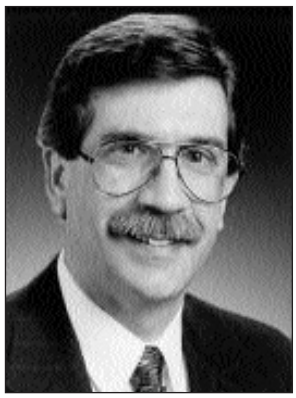
David H. Kaye is a Regents' Professor, Arizona State University College of Law, Tempe, Arizona.

Geographic Information Systems: The Wave of the Future for Information Analysis

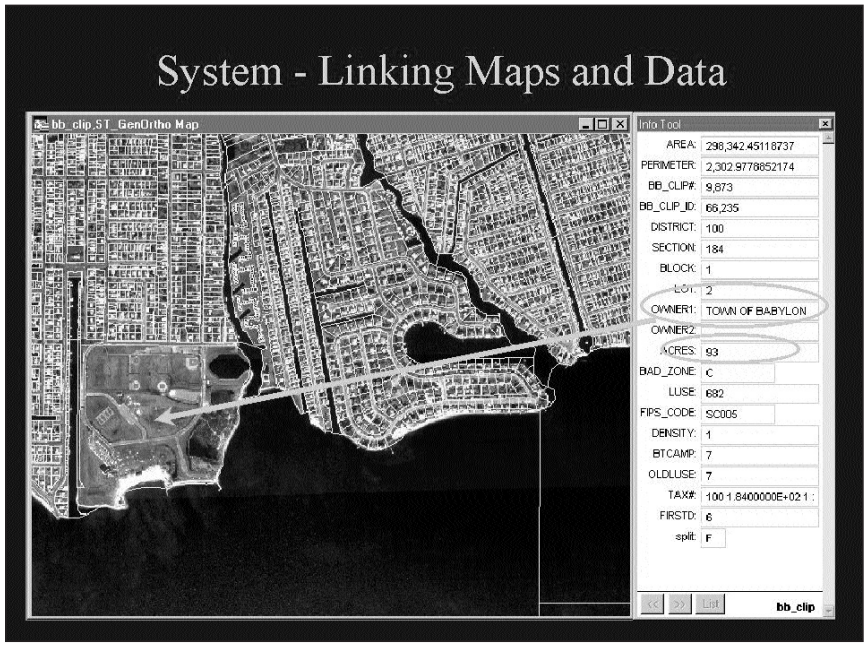
By James G. Natoli

What Is GIS?

A Geographic Information System, or GIS, as it is better known, is an electronic information system that analyzes, integrates, and displays information based on its location. GIS systems have powerful visual display capabilities that present the results of analysis on maps on a wide variety of scales. GIS is an excellent technology to understand and solve problems associated with data whose common attributes are related to place and geography.



In its simplest form, GIS can be used to create a map for the user on demand; in its more complex form, it becomes a database with millions of pieces of data that are related geographically and can be displayed in a user-friendly format to make multifaceted interrelationships visually understandable.



Although GIS is often thought of as computerized mapping, it is much more. The picture above shows digital photography with parcel boundary data outlined on top of it. The parcel data (depicted to the right) can be accessed, using GIS, by simply selecting the parcel.

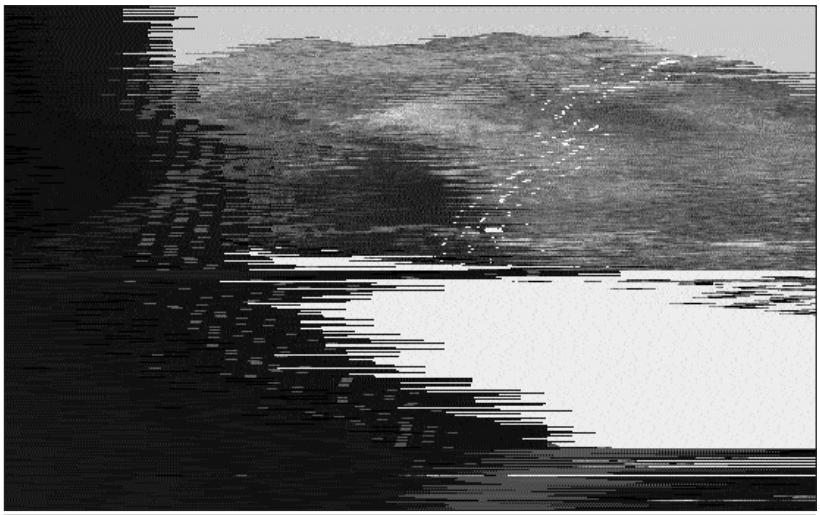
Why Is GIS Important?

GIS is no longer viewed as a complicated, expensive tool for geographers and cartographers to plot out maps. It has tremendous potential to affect a wide variety of fields, from community planning and economic development to political district mapping and criminal investigations.

In recent years, the use of GIS has grown rapidly in both the public and private sectors. While traditionally relegated to remote portions of an organization, more recently, with the advent of new products, GIS is rapidly becoming integrated into basic business applications.

Interest in GIS outside of the technology community is growing rapidly. The legal profession should also be aware of how influential this tool is, with its capacity to provide powerful visual depiction of data. In other words, managers are using GIS in their day-to-day activities.

The State of New York has taken a proactive role in recognizing the potential of GIS and working to coordinate GIS development and implementation. The State has established a framework for GIS use and collaboration not only among

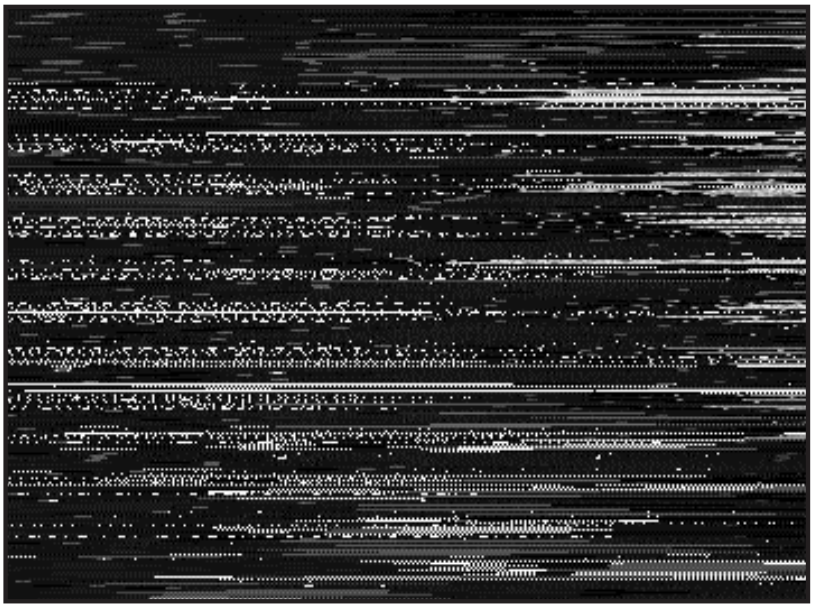


This image was provided by the Department of Transportation to the Attorney General's Office for use in defense of a major wrongful death case pending in the New York State Court of Claims. The image combines an aerial photograph draped over a 3D model of the land surface to provide a highly realistic depiction of the accident location, which occurred near the junction of a highway and the town line. The Hudson River is in the foreground in this scene looking southwest towards Storm King Mountain.

state agencies, but also with federal and local governments, other states, not-for-profit organizations, academia, and the private sector.

As GIS technology develops further, there are many issues that will need to be addressed, including defining how GIS data will be used, who will regulate it, and who will pay for it. As GIS is used more frequently in federal, state and local government, the public sector legal community will need to become aware of the implications of GIS use as it deals with licensing issues, cost and ownership rights, privacy, and confidentiality concerns.

One of the most useful features of a GIS is its ability to overlay on a map a wide variety of disparate information in order to see how these different datasets combine to answer questions and solve problems. A GIS can be used to attract new businesses by locating the most favorable sites across the State. It can show the distribution of children under age five, within the city limits, along with the location of day care providers for preschoolers. It can show the distribution of agency service centers in relationship to shifts in the population that they serve.

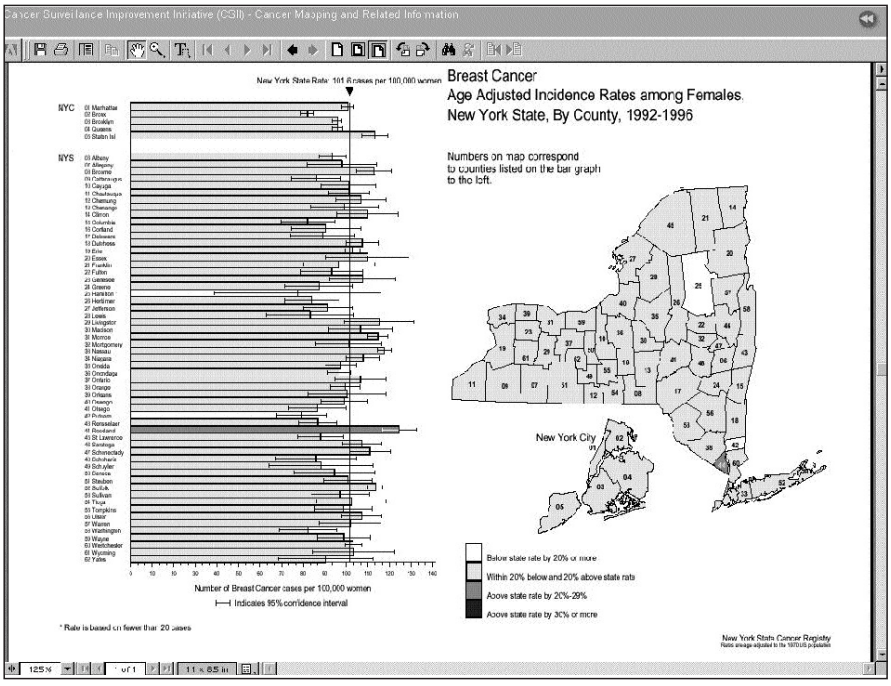


Graphic created by the Visualization Program, Center for Theory and Simulation in Science and Engineering at Cornell University.

How Is GIS Used?

The combinations of uses are only limited by the kinds of questions that need to be answered and the kind of spatial data (data that can be referenced to a street address, a census block, a highway mile marker or geographic coordinate, to name but a few methods of defining a position on the earth) that is available to answer them.

Engineers, planners, and cartographers have traditionally used GIS programs to analyze transportation systems, real property data and utility lines. Purchasing a GIS system often meant spending thousands of dollars on high-end workstations and complex software as well as training to use them. However, in the last few years, the development of PC-based and Internet GIS programs has begun to offer powerful analytical and mapping tools that are easier to use and come close to matching the sophistication of high-end tools at a fraction of the price. Program managers are starting to use these tools to analyze data and create presentations that meet their needs. Program managers around the country are recognizing GIS as a valuable tool to provide efficient and easy ways to represent, understand and solve complex problems.

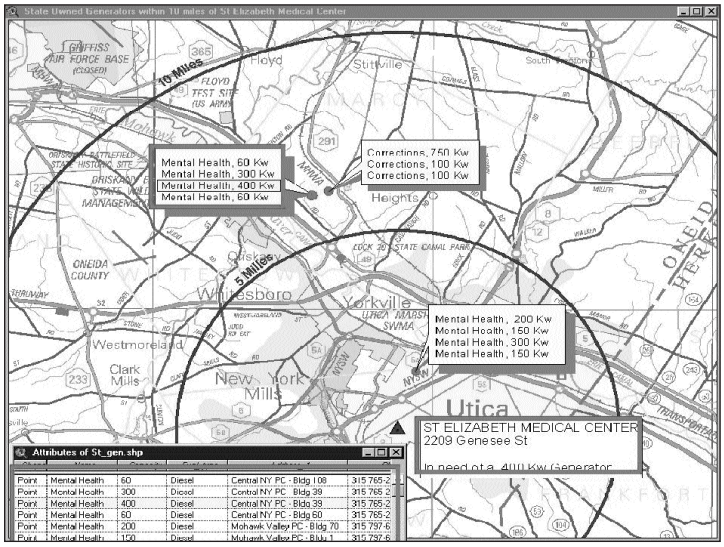


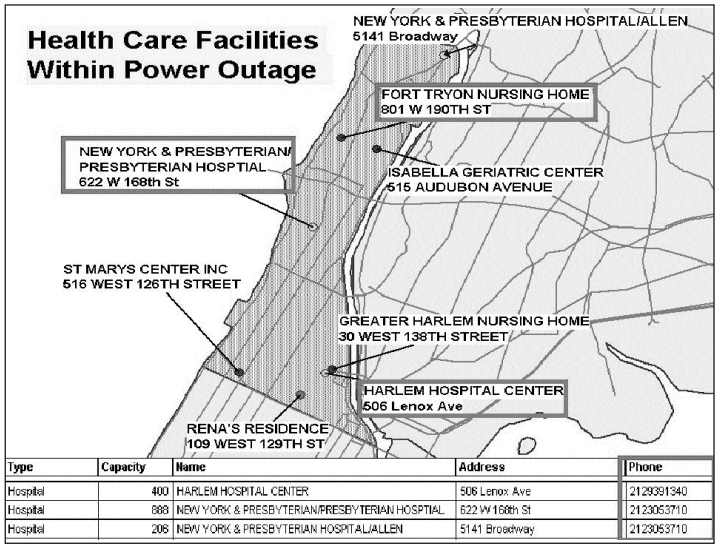
In this past year, New York State's use of GIS for health studies and emergency management has received a great deal of attention. For the first time, the Department of Health provided GIS data on cancer cases on its website. Later in the year, DOH used GIS to respond to the outbreak of encephalitis in the New York City metropolitan region.

In the past, data had to be specifically modified for GIS applications. However, due to the emerging trend of storing data in large integrated computer systems (data warehouses), the major GIS vendors are focusing on developing GIS software that will access this data without time consuming modifications. This will allow users to perform spatial analysis of existing datasets previously maintained for applications totally unrelated to GIS, thereby maximizing the value of these resources. More importantly, it provides managers with the opportunity to analyze this information using GIS tools and display it in a much more understandable visual medium.

Examples of GIS Use

GIS is recognized for its ability to assist governments in economic development, tax assessment, infrastructure management, emergency management, delivery of health and human services, planning and zoning, environmental management, transportation studies and crime analysis. The private sector is using GIS for such areas as market analysis, transportation routing, and insurance analysis.





Type	Capacity	Name	Address	Phone
Hospital	400	HARLEM HOSPITAL CENTER	506 Lenox Ave	2129391340
Hospital	888	NEW YORK & PRESBYTERIAN/PRESBYTERIAN HOSPTIAL	622 W 168th St	2123053710
Hospital	206	NEW YORK & PRESBYTERIAN HOSPITAL/ALLEN	5141 Broadway	2123053710

During 1999, GIS was used in Hurricane Floyd to locate facilities affected by power outages and flooding as well as to locate emergency generators with the closest proximity to those facilities. This capability was enhanced in preparation for potential Y2K issues.

There are almost limitless applications for GIS. Some examples are:

Economic Development. GIS offers enormous potential to support economic development. These systems can analyze locations for business expansion opportunities and can support the development and evaluation of public policies to guide expansion. A GIS can identify sites, locate customers and suppliers, and help minimize transportation and shipping costs. It can also identify workforce characteristics, educational resources, and other quality of life elements that are important to business developers. Some communities use GIS to highlight assets and attract businesses to pre-selected sites in the community using the Internet.

Environment and Natural Resources Management. Geographic information analysis allows planners and policymakers to understand the environmental effects of their policy choices. Since environmental concerns do not stop at the county line, the information needed to assess them must be shared among different jurisdictions and agencies. GIS is used in New York to support such environmental management activities as managing forests, watersheds, wildlife habitats and wetlands, as well as monitoring various sources of pollution.

Education. Schools can use GIS for such things as forecasting enrollments, optimizing bus routing and other planning needs. The box on state income tax forms that asks for a school district code is used by a GIS to help ensure that state school aid goes to the appropriate school district.

Infrastructure Management. The state's infrastructure—highways, railways, waterways, water and sewer systems, and electric, gas, telephone, and telecommunications systems—is the foundation of the state's economic development potential. The planning, design, construction, operation and maintenance of this infrastructure can be managed effectively through the use of GIS applications. For example, GIS is used in some communities to analyze the relationship between major employers, low income housing, and day care services to insure that mass transit is routed properly to service these citizens. GIS is also utilized to analyze flood zones to determine

which structures are within the 100-year flood plain and which are not. This type of information could result in a reduction of citizens' bills for costly flood insurance.

Comprehensive Planning and Zoning. Comprehensive planning and zoning are used to determine the appropriate types, intensities and locations of future developments for a community. Economic development can be balanced in this process with environmental protection, by developing strategies for the wise use and conservation of natural resources. GIS is an important tool for community planning by using inventory and analytical data of a community to simulate different program and policy scenarios in order to achieve community goals.

Real Property Records Management. Property information is the basis for maintaining, protecting and taxing property, and for planning, zoning, new infrastructure development, and the distribution of many municipal services. GIS can make property data readily accessible for economic development; allow property data to be the information base for many other uses; and can allow access to property data for such interested parties as banks, insurance agencies, real estate brokers and investors, title companies, and multiple listing services. GIS is used in some communities to provide assessors with the tools to respond to inquires quickly over the telephone, allowing assessors to save time and provide better service to citizens.

Public Health and Safety. GIS applications for public health include epidemiology, facilities siting, and health needs assessments. Public safety applications include police and fire protection and disaster mitigation. GIS also is used in some communities to review crime incidents to determine more effective routing of police patrols or relationships between the residences of past offenders and similar types of crimes. Communities are also using GIS to determine sites of recurring personal injuries and potential solutions to those problematic areas. In addition, GIS, in conjunction with 911 systems, can help determine the most effective routing to respond to emergency services.

Barriers to GIS Use

Despite the tremendous potential for this exciting new technology, there have historically been significant barriers to its widespread use. These barriers included the lack of user-friendly software, the high cost of the software (~$10,000), and availability of the data.

Nevertheless, in the last few years we have witnessed a number of developments that have positioned GIS to become a fast-growing technology:

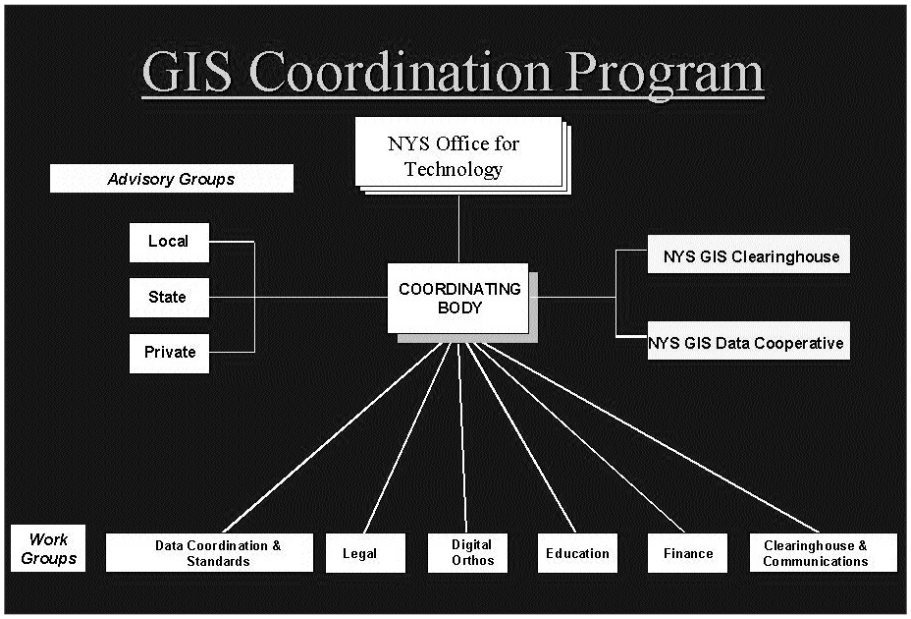
- The increase in computing power has resulted in software moving to a desktop application and no longer requiring expensive work stations to run on.
- Software designers have developed new applications geared for managers, not just for high-end users.

The New York State Temporary Geographic Information Systems Council was formed pursuant to Chapter 564 of the Laws of 1994. Its purpose was to

> examine various technical and public policy issues relating to GIS and geographic information systems and analysis; to identify the structure, functions and powers of a state-level geographic information systems coordinating body; and to examine the role a state-level body could play in assisting in the development and implementation of local government geographic information systems.

Under the statute, the Temporary Council was required to issue a report to the Governor and the Legislature that examined these issues and provided recommendations. That report was issued by the Council in March 1996. The Council's report cited a project undertaken by the Center for Technology in Government (CTG) to investigate the benefits and barriers to developing cooperative GIS efforts. CTG's report, "Sharing the Costs, Sharing the Benefits: The NYS GIS Cooperative Project" identified seven management and policy factors which hinder the sharing of spatial data:

- Lack of awareness of existing data sets;
- Lack of or inadequate metadata (information about data);
- Lack of uniform policies on access, cost recovery, revenue generation, and pricing;
- Lack of uniform policies regarding data ownership, maintenance, and liability;



- Lack of incentives for sharing;
- Absence of tools and guidelines for sharing; and
- Absence of state-level leadership.

The New York State Office for Technology (OFT), then functioning as the Governor's Task Force on Information Resource Management, was assigned the task of implementing the recommendations provided in the report. OFT's approach to problem solving was predicated on a philosophy of collaboration, not control. It was committed to fast-paced, but purposeful, change and believed that program needs drive technology, and not the reverse.[1] Because up to 80 percent of the cost of a GIS system is associated with the development and maintenance of data, OFT concentrated on the sharing and redistribution of existing GIS data as a means to have the most cost-effective impact on statewide GIS implementation.

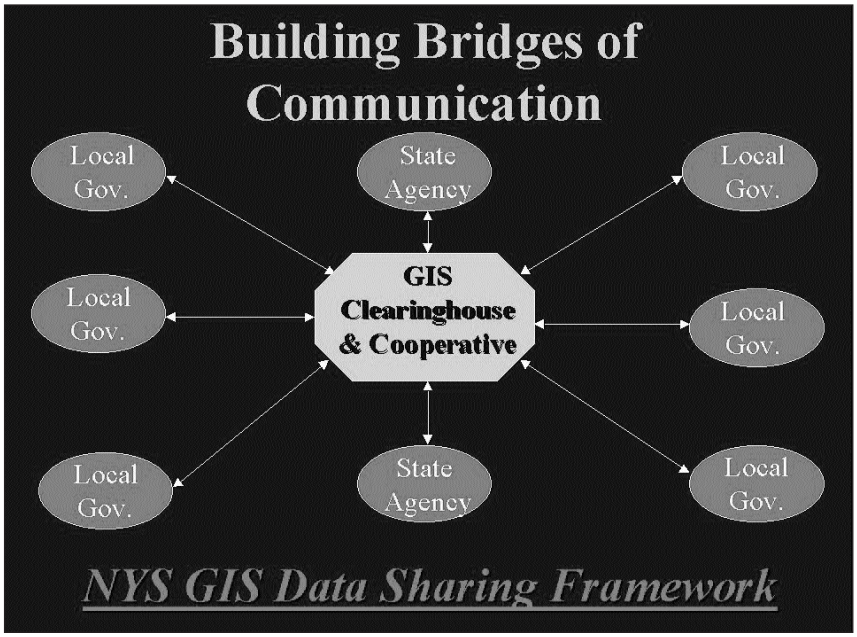
OFT began the process of coordinating a statewide GIS effort by meeting with representatives from local government, state agencies and the private sector. These groups made recommendations on a GIS Coordination Program that were incorporated into Technology Policy 96-18.[2] This policy not only established the statewide GIS Coordination Program, but also directed the development of a state policy for the easy transfer of digital GIS data at minimum or no cost.

The GIS Coordination Program is composed of various work groups of volunteer representatives from federal, state, and local governments, as well as the private sector, and started meeting in November 1996. By the first quarter of 1997, the Coordinating Body, which oversees the workgroups, had established the state's first GIS Clearinghouse,[3] and developed a concept for data sharing unique in the country. By the summer of 1997, the Clearinghouse had been totally redesigned and expanded. A new technology policy, Technology Policy 97-7,[4] required state agencies to begin sharing GIS data between themselves and with local governments through a framework known as the NYS GIS Data Sharing Cooperative.

Development of the Cooperative

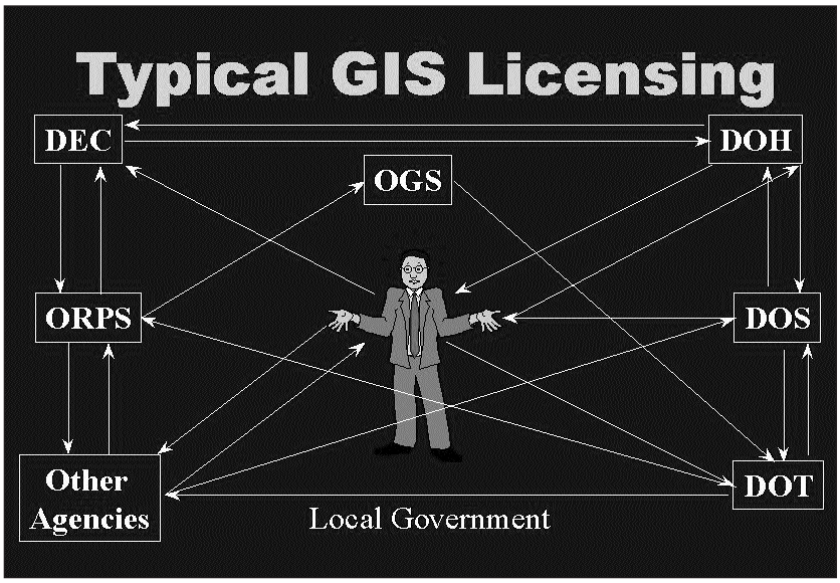
In the first few months of the NYS GIS Coordination Program, both the Data Coordination and the Legal Work Groups examined data sharing issues to arrive at a methodology acceptable to the majority of the parties involved. At that time, some state agencies used specific licensing agreements to regulate GIS data and its distribution while others distributed it upon request. Those who used licenses wanted to continue that practice, while those without licenses saw little need for it. In addition, local governments with datasets were extremely reluctant to approach this issue without the protection that licensing offered them. At the time, the New York State Department of Transportation (DOT) had the most standard license. Nevertheless, licenses took several months to negotiate with agencies wishing to share data.

As depicted below, state agencies had to negotiate licenses between themselves and local government,



In 1998, the NYS GIS Clearinghouse, combined with the Data Sharing Cooperative, was awarded the Exemplary Systems in Government Award in the National Spatial Data Infrastructure-Data Partnerships category by the Urban & Regional Information Systems Association (URISA).

therefore having to sign multiple agreements. Not only was that model cumbersome to operate within, it also was extremely time-consuming as each agency had its own nuances in each agreement.



Enter the Cooperative Concept

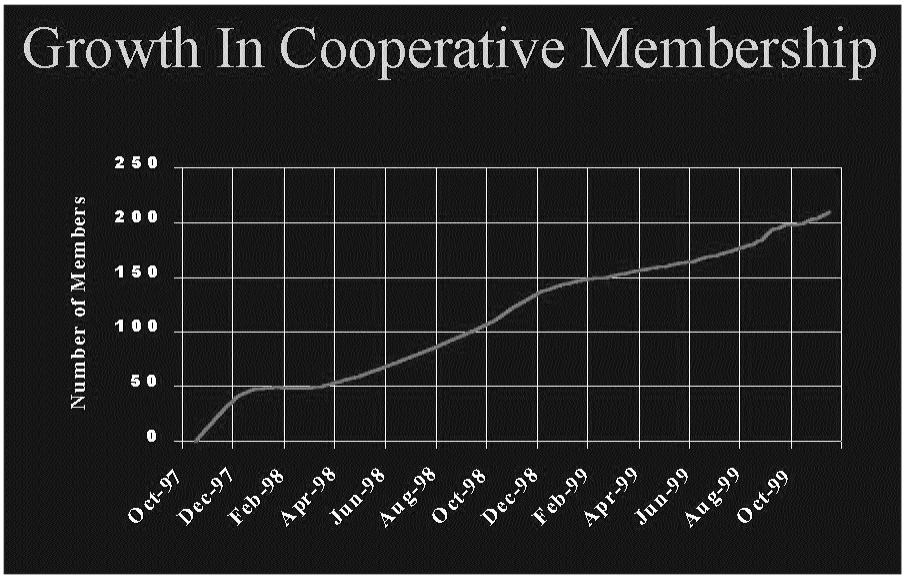
After a number of very constructive meetings, a work group composed of the major state and local government GIS data holders developed a framework through which they all could agree to share data. This framework provided rules for open GIS data sharing within an entity known as the NYS GIS Data Sharing Cooperative (Cooperative), but allowed each member the ability to distribute its GIS data outside the Cooperative in a manner in which it saw fit. Joining the Cooperative was made easy by the use of one standard Agreement.

The rules of the Cooperative are as follows:

- The Cooperative is open to all levels of government and not-for-profit corporations;
- There are no fees to join the Cooperative;
- Ownership of GIS data is not necessary to belong;
- Members can borrow GIS data from any member for no more than the cost of distribution;
- The owner of the data is free to distribute its data outside the Cooperative;
- Members sign one standard data sharing agreement to join;
- Unless required by law, members cannot redistribute another member's data without the owner's permission;
- Members borrowing data are required to forward a copy of any improvements which they make to borrowed data back to the owner; and,
- If a member is not satisfied with the Cooperative, the member simply returns the borrowed data and terminates the Agreement unilaterally.

With those simple rules, the Coordinating Body was able to obtain approval of the major state data holders as well as those at the local government level. The advantages of the Cooperative are as follows:

- Establishes a mechanism for GIS data sharing at all levels of government and eliminates the need for additional data sharing arrangements to be made;
- Provides easy access to and borrowing of GIS data;
- Avoids duplication of data development;
- Improves existing datasets; and,
- Saves money, reduces project time, and saves limited staff resources for local governments.



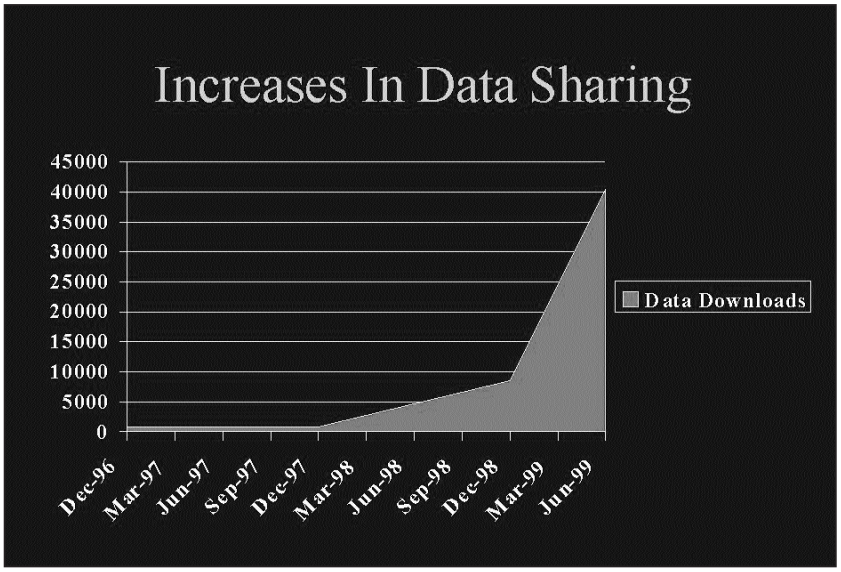
Success in the Cooperative

In establishing the Cooperative, membership began with state agencies utilizing a standard Agreement.

In March 1998, a second version of the Agreement was released for local governments and not-for-profits.[5] Later, similar versions were created and used for federal agencies and other states wishing to join. Growth in the Cooperative has been steady and currently, there are over 215 members. Members include:

- 80 State Agencies (includes 12 SUNY Campuses)
- 82 Local Governments (includes 25 counties)
- 7 Federal Agencies
- 2 States (VT & NJ)
- 48 Not-for-profits (includes 3 colleges)

More important than the number of members is the ability of this simple framework and the GIS Clearinghouse to serve as a mechanism for easy data exchange. Currently, there are over 900 datasets available to members. Of those, more than 500 are available online seven days a week, twenty-four hours a day to anyone across the state.



Through the first eight months of operation in 1998, 8,500 datasets (valued at over $2 million) were exchanged through the Cooperative, or more than 10 times the amount that occurred in previous years. Through the first six months in 1999, more than 40,000 datasets (valued at over $3.5 million) were accessed from the GIS Clearinghouse over the Internet.

Conclusion

As we move forward, the use of technology to provide solutions for government and improve business processes will increase significantly. GIS will become even more integrated into the public and private sectors as a means to improve services and save money. GIS has the potential for a wide impact across public and private sectors. There are many different parties that have a stake in GIS, and any guidelines or rules established should address the needs of all involved. By working collaboratively, the technology and legal communities can succeed in making GIS a powerful tool.

In collaboration with:

William F. Pelgrin, Executive Deputy Commissioner and Counsel for NYS Office for Technology;

Bruce Oswald, Project Director, NYS Office for Technology;

Krista Montie, Executive Assistant, NYS Office for Technology.

Bibliography

Center for Technology in Government, *Sharing the Costs, Sharing the Benefits: The NYS GIS Cooperative Project*, 1995

New York State Office for Technology GIS Clearinghouse, *Executive Briefing*, 1996

New York State Office for Technology, *Technology Policy 96-18, Geographic Information Systems*, 1996

New York State Office for Technology, *Technology Policy 97-6, GIS Data Sharing*, 1997

New York State Office for Technology Web site: http://www.oft.state.ny.us

New York State Temporary Geographic Information Systems Council, *Geographic Information Systems: Key to Competitiveness*, 1996

Oswald, Bruce, *NYS Lowers the Barriers to GIS*, 1999

Visuals:

Cornell University, Center for Theory and Simulation in Science and Engineering

NYS Department of Health

NYS Department of State

NYS Department of Transportation

NYS Y2K Emergency Preparedness Task Force

Endnotes

1. For more information about OFT, visit its website at http://www.irm.state.ny.us.
2. Http://ww.irm.state.ny.us/policy/tp_9618.htm.
3. Http://www.nysl.nysed.gov/gis.
4. See website, http://www.irm.state.ny.us./policy/tp_976.htm.
5. A sample of the local government Agreement is available on the GIS Clearinghouse at: http://www.nysl.nysed.gov/gis/coop.locldata.htm.

James G. Natoli, Director of State Operations, is responsible for the day-to-day direction of all state Departments and Agencies. Mr. Natoli serves as Chairman of the Governor's Office for Technology.

Technological Innovations in Court Administration in the New Millennium—The Advent of Filing of Court Documents by Fax or Electronic Means

By Amy S. Vance

With the dawn of the new millennium, it is worth asking "How will the technological revolution, particularly the availability of the Internet, affect court administration in the ensuing decade?" Many changes in technology are already taking place that will improve the practice of law. Once inaugurated, these changes have the potential to significantly alter the way law is currently practiced. One of the most significant changes contemplated is permitting lawyers or self-represented parties to initiate lawsuits and subsequently file court papers by fax or electronic means.

The New York State Unified Court System (UCS) has been exploring the possibility of permitting the filing of court documents by fax and electronic means in several pilot sites for more than two years. It reviewed the status of fax and electronic filing initiatives across the country, studying particularly closely the experiments in the federal court system, which is somewhat more advanced than most state court systems. It consulted widely within New York State as well, asking the Chief Administrative Judge's Advisory Committee on Civil Practice to recommend the statutory and regulatory changes needed to permit such pilots, and obtained advice from an in-house steering committee of court-related personnel (comprised of judges, court attorneys, court clerks, county clerks, and senior UCS staff), and an advisory committee of lawyers from major bar associations, large institutional litigants, and lawyers from the locations where the pilots would take place.

In 1999, at the urging of the judiciary, the New York State Legislature enacted Ch. 367 of the Laws of 1999[1] authorizing the Chief Administrator to undertake an experimental program in which actions and special proceedings may be commenced and subsequent papers served by facsimile transmission ("fax") or electronic means in selected courts for certain limited case types. The courts selected for the experiment are the Supreme Courts of Monroe, New York, Westchester, and Suffolk Counties and the New York Court of Claims. The cases subject to filing by fax will be limited to commercial claims in the New York and Monroe County Commercial Divisions; mental hygiene, conservatorship proceedings, and tax certiorari claims in the Suffolk County Supreme Court; and claims against the State of New York in the Court of Claims. The cases subject to filing by electronic means will be limited to those involving tax certiorari claims in Westchester County Supreme Court, and commercial cases filed in the Commercial Divisions of the Monroe and New York County Supreme Courts. It is anticipated that any necessary fees will be paid by credit card or other electronic payment devices authorized by the Chief Administrator. Participation in the program will be strictly voluntary, and will only take place upon the written consent of all the parties and the judge assigned to the case.

The UCS believes that the filing by fax and electronic means will bring numerous benefits to the courts, litigants, attorneys, and the public alike, and make the courts more user-friendly. The filing by fax program will save attorneys and self-represented litigants the time and expense associated with personally filing court papers. The filing by electronic means will provide even greater benefits. Most costs associated with paper handling and storage will be eliminated; case materials will be instantly accessible and protected from loss or destruction; productivity will be enhanced; attorneys will no longer have to bear the time and expense of sending documents to the courthouse, and will have access to case files anytime of the day or night.

The Chief Administrator issued regulations governing the experiments in October 1999[2] and it is anticipated that the new programs will be in place by June, 2000.[3] Here's how the new systems will work. First, a discussion of the fax option is in order. Papers in any covered civil action or proceeding, including those commencing an action or proceeding, may be filed with the appropriate court clerk by facsimile transmission, at a designated 800 number provided by the court for that purpose. The cover page of each facsimile transmission in a form prescribed by the Chief Administrator, will be attached and will state the nature of the paper being filed; the name, address and telephone number of the filing party or party's attorney; the facsimile telephone number that may receive a return facsimile transmission, and the number of total pages, including the cover page, being filed. Whenever a paper is filed that requires the payment of a filing fee, a separate credit

card or debit card authorization sheet will be included, containing the credit or debit card number or other information of the party or attorney permitting such card to be debited by the clerk for payment of the filing fee. The card authorization sheet will be kept separately by the clerk and will not be a part of the public record. The clerk will not be required to accept papers more than 50 pages in length, including exhibits, but excluding the cover page and the card authorization sheet. The court system's centralized server will route the fax to the proper court where it will appear on the computer screen of the appropriate clerk.

Papers may be transmitted at any time of the day or night and will be deemed filed upon receipt of the facsimile transmission; provided, however, that where payment of a fee is required, the papers will not be considered filed unless accompanied by a completed credit card or debit card authorization sheet. The clerk will date-stamp the papers with the date that they were received, and where the papers initiate an action, will also mark the papers with the index number. No later than the following business day, the clerk will transmit to the sender a copy of the first page of each paper, containing the date of filing and, where appropriate, the index number, to the filing party or attorney, either by facsimile or first class mail. If any page of the papers is missing or illegible, the clerk will notify the party or attorney, and the party or attorney must forward the new or corrected page to the clerk for inclusion in the papers.

Attorneys who wish to serve papers upon another attorney or party will continue to be able to do so pursuant to CPLR 2103(b)(5), as long as the other party consents (which can be done by simply listing a fax number on the attorney's letterhead) and a hard copy of the paper is also mailed to the fax recipient.

Service of court papers by electronic means will be slightly more elaborate. In order to participate, an attorney must have a personal computer, a modem connecting the computer to the Internet, an Internet browser (Netscape Navigator or Microsoft Internet Explorer), and software entitled "Adobe Acrobat Exchange," which creates a "portable document format" or a "pdf" file. This software essentially takes a picture of the word processed document before it is sent over the Internet so that it cannot be altered. The software costs approximately $95. A scanner will be useful as well since some documents, such as exhibits, must sometimes be scanned into the computer since they were not created as a word processed file.

If an attorney wishes to participate in the experiment, he or she must first register with the court system as a designated "Filing User." Attorneys admitted to practice in the State of New York will be eligible, as well as attorneys admitted *pro hac vice* for the purposes of the action. Self-represented parties will be eligible for Filing User status as well. Once the attorney or party sends in the registration form and is approved, he or she will be given a password and a Personal Identification Number (PIN). These two items, when submitted together, will become the electronic signature of the participant.

The Filing User will then draw up the documents he or she wishes to file in an authorized case and will file the documents over the Internet, by means of a new UCS website, which will be attached by hyperlink to the current UCS home page found at <www.courts.state.ny.us.> Let's say, for example, that the attorney wishes to commence a lawsuit. He or she will use an Internet browser to access the website, and click on the option "Commence an action or proceeding." The sender will fill out necessary background information, such as the Filing User status, convert the documents through a few more clicks to a "pdf" file and then double-click to send the documents over the Internet to the website, which will serve as the filing locus for both the county clerks and the supreme court clerks in the counties participating in the experiment.

As with fax filing, papers may be transmitted at any time of the day or night to the UCS Internet site, and will be considered to be filed upon the receipt of those papers by that site; provided, however, that where payment of a fee is required, the papers will not be deemed filed unless accompanied by a completed credit card or debit card authorization sheet. Within 24 hours, the county clerk will return a confirmation of filing by e-mail, together with the first page of the document stamped with the index number. If the county clerk finds a defect in the document, he or she will notify the filing party within 24 hours so that they will have an opportunity to correct their papers.

The new system will add another service option for obtaining personal jurisdiction. The new rules still permit the attorney or party seeking to effect service to obtain personal jurisdiction to serve by any of the other methods currently permitted by Article III of the CPLR; however, they will also now allow service of the opposing party by electronic means if he or she agrees to accept service by this method. The party that agrees to accept service by electronic means must provide the serving party or attorney with an electronic confirmation within 24 hours of service that the service has been effected.

When the party commences a lawsuit and first serves his adversary, he or she must include a Notice of Availability of Electronic Filing, to be supplied by the county clerk, which will provide information on the experimental program and encourage attorneys and parties to participate. If the opposing party agrees, he or she will file a formal consent to Filing by Electronic

Means ("FBEM")with the Court, together with a Request for Judicial Intervention ("RJI"). The parties will supply the court with a list of all e-mail addresses of record, which will be placed on the website. If the judge assigned to that case elects to participate in the FBEM program, the clerk will notify the parties, and the judge will issue a formal order designating the matter as an FBEM case. Once an action is designated as being subject to FBEM, all papers must be filed electronically, and the electronic file will become the official record.

The new rules do, however, permit the judge to terminate or modify the application of FBEM to an action, or excuse a party from compliance with any provision of these rules in order to prevent prejudice and promote substantial justice. This is only likely to happen in cases where there is third-party practice and the third party defendant has little computer equipment or experience and feels uncomfortable using FBEM, or an intervenor comes into the case with the same apprehension. In that case, the judge can modify the original order to require service of papers on the party that declined the FBEM option to be served in hard-copy form.

Service of interlocutory papers in an FBEM case will also be different from the current practice. An attorney or party filing an interlocutory paper pursuant to FBEM procedures must first file the document electronically with the court, and will then receive an automatic, computer-generated confirmation of electronic filing from the court. The serving party will then send electronically a notice of filing of the paper to all e-mail addresses of record. The notice will provide the electronic document number and the title of the paper filed, and the date and time the document was filed, as set forth in the confirmation of filing. Then, it will become the responsibility of the other party to access the UCS Internet site to obtain a copy of the actual paper which was filed. The electronic transmission of the notice of filing will constitute service of the paper on the addressee. If the filing party wishes to utilize existing service methods, such as mail or personal delivery, to serve the opposing party, after electronically filing the document with the court, he or she will still be able to do so.

The experimental program does not contemplate the electronic filing of discovery documents. This will only be done if the parties stipulate that they wish this to happen and the court, by order, concurs. Under the experiment, submissions pursuant to FBEM will have the same copyright, confidentiality, and proprietary rights as paper documents. If a party, or even a non-party, is concerned about the potential abrogation of those rights in any action subject to FBEM, he or she may apply for an order prohibiting or restricting the electronic filing of specifically identified materials on the grounds that such materials are subject to copyright or other proprietary rights, or trade secret or other privacy interests, and that electronic filing in the action is likely to result in substantial prejudice to those rights or interests.

The Chief Administrative Judge plans to monitor this experiment closely, making any needed changes in procedure or the regulations as soon as they are indicated, and will file a complete report evaluating the pilot with the Chief Judge, the Governor, and the leaders of the Legislature by April 1, 2002, as the implementing legislation requires. Since the current law has a sunset provision and will be no longer effective as of July 1, 2002, it is anticipated that any new legislative changes will be recommended by the UCS during the 2002 legislative session. If the pilot program is deemed a success, the Chief Administrator will consider expanding it to other courts and case types, keeping in mind the special privacy and confidentiality considerations of matrimonial and family court cases.

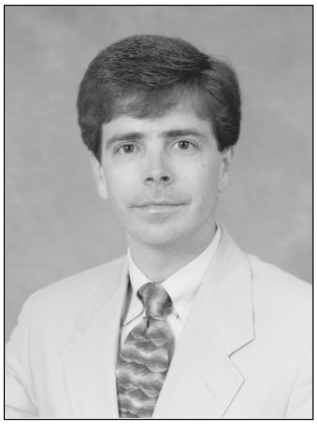
Endnotes

1. This bill amended the sections of the Civil Practice Law and Rules dealing with the commencement of an action or special proceeding (§ 304), the form of papers (§ 2101), and the service of papers (§ 2103). It also created a new § 8023 of the CPLR and amended Judiciary Law § 212(2)(j) to deal with the payment of certain court fees by credit card.
2. See New York Uniform Rule Pt. 202.5.
3. The Court of Claims already commenced its program, starting May 1, 1999, and the Suffolk County Supreme Court began its experiment in July, 1999.

Amy S. Vance, Esq., is Deputy Counsel to the New York State Office of Court Administration, and serves as Counsel to the Chief Administrative Judge's Advisory Committee on Civil Practice.

Legal Resources on the Internet: A Practitioner's Guide

By Kirk Lewis



The impact of the "information revolution," and more specifically the Internet, on traditional methods of storing and maintaining legal information, is just beginning to be realized. Case reporters and statutes, the traditional repositories of the basic tools of the lawyer, were first challenged by the paid search services, Lexis and Westlaw. The next wave of change came with the CD-ROM, with its capability to store vast amounts of digital information. Law librarians suddenly had the option of replacing a multi-volume series of case reporters with one or two compact discs and a computer equipped with a CD drive. Most recently, the widespread availability of the Internet, coupled with technology advances that permit the storage and transmission of greater amounts of digital information, have greatly increased the resources that are available on web sites. This latest evolution mirrors a trend in other areas, in which applications and data are available on the Internet, and accessed from remote computers, rather than being stored and maintained at the work site.

As an attorney who has moved from a private practice, with a well-supplied library, to being general counsel for a private, non-profit human service organization with very few traditional legal resources, I have sought to exploit as fully as possible the range of resources that are available on the Internet. In the past year I have found numerous resources available that have minimized the need for me or my employer to invest extensively in developing a more "traditional" library. Indeed, given the rapid evolution of methods of information storage and retrieval, it is clear the law library of the future will look nothing like the traditional library of the past, and may, in fact, reside on the lawyer's desktop. As the foregoing discussion demonstrates, there already are a vast number of resources available to attorneys from non-traditional sources. For government attorneys, attorneys working for non-profit organizations, or anyone with an eye on the expense of maintaining a traditional library, the Internet is a great source of information. The following is a summary of the resources that I have found to be most useful on a regular basis.

News Sources

While in private practice, I tried to review the *New York Law Journal* on a daily basis, although the time demands of daily practice sometimes resulted in piles of *Journal*s accumulating in the corner of the office. Even a review of the headlines, however, provided news as to current developments, and pointed me to information (such as changes in procedural rules or significant case law) that I would get to later. There are several sources available on the Internet that are extremely informative, and many of them are free. First, I have the home page for my web browser set for the *New York Law Journal*'s website, <http://www.nylj.com.> This site is similar to the front page of the paper *Journal*. There are headlines and summaries for five to seven stories, as well as links to the "Decision of the Day" and a variety of other decisions from both the state and federal courts. There are extensive links to other law related sites and to stories within the *Law Journal*'s site. One interesting feature is the listing of links to law firms mentioned in that "issue" of the *Journal*: clicking on the link brings you to the story in which the firm is mentioned.

Another source for daily legal news is a free subscription service provided by American Law Media that I receive by e-mail each day. This service, which appears in my e-mail in box as "Law News Network," transmits an HTML (hyper text markup language) file that contains summaries of legal stories from around the nation. The summaries are linked to the full stories at their source. In addition, the site has links to specialty areas, such as employment law, technology trends, employment resources, and chat rooms targeted at lawyers. The Internet version of the News Wire can be found at <http://www.lawnewsnetwork.com/newswire/index.html>; from this site, you can subscribe by providing an e-mail address so the news wire will be sent to you on a daily basis.

There are numerous other sources for news on the web. Most local papers now have web sites (for example, for Albany news the Albany *Times Union* has a very "user friendly" site at <http://www.timesunion.com>; for more comprehensive coverage, the *New York Times* has a site, <http://www.newyorktimes.com>, which requires registration but is free). For legal news, however, I have found that the two sites discussed above provide excellent summaries of current legal news, on both a state and national level, together with the links to more detailed stories if I wish to pursue them.

General Legal Information

There seems to be an ever-increasing number of sites that contain a great deal of information aimed at the legal profession. Some of these are commercial sites, while others are sponsored by law schools or bar associations. I have found these sites to be invaluable, and I have several bookmarked to use as starting points for legal research. One of the first sites that I learned of, and one of the best, is the site maintained by Cornell University School of Law. This site, known as the "Legal Information Institute," or LII, is found at <http://www.law.cornell.edu.> For the New York practitioner, the links and data available from site are excellent. From the home page, users can go to decisions from the Court of Appeals and the United States Supreme Court. These databases are searchable, which makes them particularly useful to the attorney who does not have ready access to case law indexes or annotations. The Cornell site contains links to statute and case law databases across the country, along with information about new sources available on the Internet. Finally, the LII publishes a summary analysis of Court of Appeals decisions that it calls the Bulletin, which it distributes, free of charge, to subscribers to the service. Similar to case notes published in law reviews, the LII summaries (which are prepared by law students) provide a summary of the facts, the legal issues, and a brief analysis of the decision (and the dissent, if any). Information about the Bulletin, including how to subscribe, and links to past editions, is available at <http://www.law.cornell.edu/bulletin/>. In general, the Cornell site has been an excellent resource.

Another excellent resource is the New York State Bar Association's web site (<http://www.nysba.org>). Not surprisingly, this site has a wealth of information about Bar Association activities, including legislative news, press releases (and information on electronically subscribing to those releases), and information about the activities of the sections and the committees. In addition, this site has information about the new Continuing Legal Education requirements, with links to the rules and information about the many CLE courses sponsored by the State Bar. The site also has many links to other sources of legal information on the web. One of the most comprehensive collections of links to law-related web sites is contained on the web site sponsored by the Committee on Attorneys in Public Service (the Committee that publishes this *Journal* in conjunction with the Government Law Center of Albany Law School). This site can be accessed through the State Bar's home page (by clicking on "Committees," and then going to the link to the Committee on Attorneys in Public Service), or reached directly at <http://www.nysba.org/committees/aps/default.htm>. The "Legal Links" section of this site contains listings for seven comprehensive legal sites, seven federal law sites, 11 New York State sites, and a variety of other links. This site will also link to paid services, such as Westlaw or Lexis, if the user has an account. This site has been particularly useful as a starting point for searches that may go in several directions.

A commercial site with very broad coverage is the FindLaw site (<http:www.findlaw.com>). This site, which is searchable, has data organized by legal topic, by source (i.e., case law or statute), and by location (federal, state or foreign). It also links to sites with information about law schools, professional development, consultants and expert witnesses, and practice materials. Finally, there are numerous links to commercial sites, message boards, and web search engines (Excite and Alta Vista). Although there are many other sites that have general coverage (see, for example, the list in the "comprehensive" category of the legal links in the Attorneys in Public Service web site), I have found that the sites cross-reference each other extensively, and tend to rely on the same basic data sources. Thus, if I am searching for a source and I haven't found it on one of these sites, I will usually continue my search at a more traditional venue (such as a law school library).

Statutes and Case Law

Although the comprehensive sites provide good starting points to get to a variety of sources, I have several sites that I rely on for basic data such as New York statutes, federal statutes, or New York case law. For New York statutes, both the state Senate and Assembly have sites that include links to New York's Consolidated Laws, Unconsolidated Laws, the Constitution, and current session laws. The Assembly's site is at <http://assembly.state.ny.us/>: to get to the laws, click on "Assembly Legislative Information System," and then select New York State Laws. This site will also give you information about current legislation and hearings. Similarly, the Senate site, at <http://senate.state.ny.us/>, has links to the full text of New York laws, as well as information about legislation, senators, and activities of the senate. I have found both of these sites very easy to use: the laws are compiled in a "gopher" menu, which permits the user to click on the desired title (e.g., "Mental Hygiene Law"). This brings up a list of articles (or, in the Senate menu, a list of every section). Clicking on the desired article will bring up either a table of contents for the article, or a list of the sections. Clicking on the desired section will bring up the full text of the law, together with information about amendments. Both of these sites put the full body of New York statutory law before you in a very accessible format.

Missing from these sources, of course, are the helpful case law annotations found in McKinney's and the CLS collections of New York Statutes. Although not a complete substitute, I have found a free searchable

database of New York case law that is an excellent resource. The site at www.Jurisline.com allows you to select a jurisdiction and then search its database of cases for that jurisdiction. The page on which search queries are formulated is extremely easy to use: in addition to having good examples of how to formulate a search, there is a form that can be filled in to add restrictions to a search, such as date, parties, or judges, without complicating the query. Although I have never been comfortable relying on a computer search as an exhaustive review of case law, this service is an excellent way to get started. Also, because you can search by citation, it is an efficient way to read cases that you might otherwise need to go to the library for.

If you are only looking at cases from the Supreme Court or the Court of Appeals, the LII site sponsored by Cornell is another way to gain access to this information. These databases also are searchable.

Another searchable database that I have used frequently is the collection of the Code of Federal Regulations (CFR), at a site that is maintained by the United States Government Printing Office, the National Archives and Record Administration, and the Office of the Federal Register. The web address for the starting point for the searchable database is <http://www.access.gpo.gov/nara/cfr/cfr-table-search.html>. Given the fact that I have never found the paper edition of the CFR to be particularly user-friendly, I have been impressed with my ability to locate sections and provisions using the search tools provided by this site. Like any search engine, the more you use it the more comfortable you become with its particular features. One way that I test my ability to use a searchable database is to try a word search for a provision that I know is in the law if I cannot locate something that I know is out there, I will either try to relearn the search engine, or find another database!

Although most of my federal research has been confined to the CFR, the United States Government Printing Office web site has a wealth of other legal information. From the GPO home page at <http://www.access.gpo.gov>, you can link to the United States Code, the Federal Register, and to sites relating to most federal agencies and commissions.

Finally, this review would not be complete without mentioning the sites maintained by many New York State agencies. For example, the Department of State's site (<http://www.dos.state.ny.us>) has information about all of the functions of the department, together with an ever-growing number of forms that can be downloaded to facilitate filings. I have bookmarked this site, as it has links to several other useful New York sites, including the New York State Government Information Locator (http://www.nysl.nysed.gov/ils/), which describes itself as "a single point of access to information services provided by New York State government agencies, the State Legislature and the Judiciary." These sites have provided me with quick access to the extensive information available on the Internet from state government.

The options available to the legal profession and the public for access to legal information are vast, and they are growing rapidly. Possibly the biggest surprise for me, in leaving private practice, is how readily and efficiently the Internet could replace the traditional law library. Although it seems likely that the traditional library will continue for the foreseeable future, it is clear that both the public and the profession will benefit from the increasing availability of legal resources on the Internet. As the resources continue to expand, the biggest challenge will be keeping current both with the resources, and with the technology needed to access the resources.

Kirk Lewis, Esq., is the general counsel to Schenectady County Chapter, NYSARC, Inc. He was formerly in private practice.

Techno-Ethics in New York State Government Under the Public Officers Law

By Donald P. Berens, Jr.

Introduction

In keeping with the theme of technology in government, this article will focus on four otherwise unconnected ethical questions with a common technological flavor. The first two are hypothetical; they are answered by analysis of regulation and statute without any precedential advisory opinions on which to draw. The others are real and have been answered by the New York State Ethics Commission in formal opinions. The first concerns sales of website advertisement brokerage services to State agencies by a State employee moonlighting as a private entrepreneur; the second, services offered to a State agency by a retired computer programmer; the third, work by a former State scientist for a private company to develop a vaccine technology discovered by him and patented by the State; and the fourth, work by a current State scientist as a consultant to a pharmaceutical company funding research at a State laboratory.

The Cyber-Entrepreneur

QUESTION: May a New York State employee, who moonlights as a broker of website advertisements, arrange for the placement of advertisements on a State agency website in return for a percentage of the fee paid by the advertiser to the State? Does it matter whether the employee's agency is the one selling website space? Does it matter what the employee's State duties are? Does it matter how much the employee is paid to perform his brokerage business in general or to place the particular advertisement on the State website? Does it matter if the employee's fee is a fixed amount or a percentage commission?

ANSWER: This cluster of questions requires analysis of one general statute, two specific statutes and a regulation. It may require review of any applicable agency code of ethics. These authorities are designed to limit the opportunities for current State employees to misuse their public position for improper private gain, or to appear to do so.

The general statutory rule with respect to conflicts of interest is that no State officer or employee should have any interest, financial or otherwise, direct or indirect, or engage in any business or transaction or professional activity or incur any obligation, in substantial conflict with the proper discharge of his or her duties in the public interest.[1] This statute is supplemented by an Ethics Commission regulation. Any State officer or employee, whether or not policy-making and whether or not paid, should avoid any outside activity which interferes or is in conflict with the proper and effective

discharge of the individual's official duties or responsibilities.[2]

One specific statutory prohibition concerns contingent fees. No State officer or employee shall receive or agree to compensation for services to be rendered in relation to any matter before any State agency where the compensation is to be dependent or contingent upon any action by such agency.[3]

A second specific prohibition concerns sales to State agencies. No State officer or employee (or firm or association or corporation 10% or more of the stock of which is controlled directly or indirectly by such person) shall sell any goods or services worth over $25 to any State agency unless they are provided pursuant to an award or contract let after public notice and competitive bidding.[4]

Based on these statutes, a State employee engaged in website advertisement brokerage transactions should not sell such brokerage services worth more than $25 to any State agency without public notice and competitive bidding. The Ethics Commission has issued no formal Advisory Opinion concerning the receipt of contingent fees, but it appears that the employee's compensation should not depend on the decision of a State agency to accept advertisements; however, a fee based upon the reasonable value of the brokerage services is not prohibited. And if the employee's public duties might appear to conflict with his private activity (for example, if he contemplates brokering advertisements to be placed on the website of a State agency where he is the webmaster or the procurement officer), then he should consult the agency ethics officer or the Ethics Commission for confidential advice before proceeding. The agency ethics officer will know if there is any agency code of ethics supplementing the Public Officers Law.

The above authorities apply to all State officers and employees as defined in the Public Officers Law. Policymakers are subject to additional regulation as well.

The New York State Ethics Commission restricts by regulation the ability of State officers and employees to engage in certain outside activities.[5] An individual who serves in a policy-making position on other than a nonpaid or per diem basis needs the prior approval of the

Commission in order to engage in any private employment, profession or business, or other outside activity from which more than $4,000 in annual compensation is received or anticipated.[6] Such a paid policymaker also needs Commission approval to serve as a director or officer of a for-profit corporation or entity.[7] Even if he anticipates less than $4,000 in annual compensation, if he receives or anticipates more than $1,000, he needs prior approval of his "approving authority."[8] For most State employees, the approving authority is the head of the employing State agency or the head's designee; for some, it is the Commission.[9]

Based on the regulation, a salaried policy-making State employee who anticipates earning more than $1,000 from such website advertisement brokerage activities should obtain prior written approval, and should consult the agency ethics officer or the Ethics Commission to determine who must approve. A policy-making State officer who is either not paid or paid on a per diem basis should consult the agency officer or the Ethics Commission to see how any agency code of ethics might apply.[10]

If the State employee receives annual income in excess of $1,000 from a single source, such as a firm engaged in website advertisement brokerage, and if he is a policymaker or high-paid employee who is otherwise required to file an annual statement of financial disclosure, then he must report that income on the financial disclosure statement.[11]

The Returning Programmer

QUESTION: May a computer programmer who retired from State employment, either contract individually, or be a member or employee of a firm, corporation or association which contracts, to render services to a State agency to reprogram its computers so that they are Y2K compliant? Does it matter whether the retiree's former agency is the one seeking the services? Does it matter what the retiree's former State agency duties were? Does it matter if the former employee personally appears at the State agency or instead confines the services to off-site locations?

ANSWER: There are two "revolving door" rules and an exception to consider. The revolving door rules are intended to limit the opportunities of State employees to perform their official duties in such a way as to improperly benefit themselves when they leave public service or, after leaving, to use their State contacts or inside information for unfair private advantage.

Generally, a former state employee during a period of two years after her departure from State service, is barred from appearing before her former agency or receiving compensation for services in relation to any matter before that agency.[12] Also, a former State employee throughout her lifetime usually is barred from appearing before any State agency or receiving compensation for services in relation to any case with which she was directly concerned and in which she personally participated while in State service.[13]

Under the usual rules, the former employee's duties are an important factor in analyzing the application of the lifetime bar, but not the two year bar. The identity of the former agency is critical for the application of the two-year bar, but not the lifetime bar. And the performance of compensated "back room" services, without a personal appearance by the former employee, can be barred under either the two-year or the lifetime bar.

Former employees are subject to both the two-year and lifetime bars. However, the revolving door rules do not prohibit a firm, association or corporation of which the former employee is a member, associate or shareholder, from appearing, practicing, communicating or otherwise rendering services in relation to any matter before a State agency, where the former employee does not share in the net revenues resulting therefrom.[14]

However, notwithstanding the general two-year and lifetime bars, a former State employee may contract individually, or as a member or employee of a firm, corporation or association, to render services to a State agency when the agency head certifies in writing to the Ethics Commission that the services of the former employee are required in connection with the agency's efforts to address the State's year 2000 compliance problem.[15]

The Inventive Scientist

QUESTION: A scientist, while employed by the State, developed technology the patent rights to which he assigned to the State. More than two years after leaving State service, may he work for a business corporation to develop that same technology for commercial use with State permission? Does it matter whether the State assigned to the corporation the patent rights which were to be developed in a joint venture controlled indirectly by the State or instead licensed the use of the technology by the corporation?

ANSWER: The application of the lifetime bar to a particular "case, proceeding, application or transaction" is heavily dependent on the specific facts.

No person who has served as a State employee shall after the termination of such employment receive compensation for any services rendered by him in relation to any case, proceeding, application, or transaction with respect to which he was directly concerned and in which he personally participated during the period of his State service, or which was under his active consideration.[16]

The Ethics Commission has considered these questions in the case of "Dr. X," who had been a Research Scientist for the State Department of Health (DOH) and its closely affiliated not-for-profit research corporation,

Health Research, Inc. ("HRI"). During his DOH employment and while working in his field of lifelong expertise, Dr. X discovered a vaccine technology. DOH acquired the patent and assigned those rights to HRI with the intent that the private sector would commercially develop the technology, because DOH and Dr. X lacked the capital and ability to develop marketable products using the technology. DOH, HRI and a pharmaceutical corporation entered a joint venture which created a new company which hired Dr. X to help develop the technology. Dr. X directed the new company's research toward both developing marketable products and understanding the particular virus at issue.[17]

The Commission determined that Dr. X's research for the new company was not in relation to any particular case, proceeding or application, much less one in which he had participated while in State employment. It considered whether his new work was impermissibly related to an old transaction. The Commission cited prior opinions in which it had held that it is permissible for former employees to draw on their knowledge of old transactions if the information bears a relationship to current transactions[18] and that the lifetime bar does not preclude a former State employee from rendering compensated services on new and separate transactions, even if the employee may have been directly concerned or personally participated in a similar or related transaction while in State service.[19] The Commission refused simply to exempt Research Scientists from any lifetime bar provisions. The Commission determined that Dr. X's current scientific work was not barred because it was not the same as any transaction on which he had worked for the State. The determination was based on the specific, perhaps unique, circumstances of Dr. X's case: the technology was his lifetime work, begun long before his DOH employment; DOH had specifically negotiated his transfer to the new company in furtherance of DOH's goal of applying the technology to marketable vaccines; and DOH and HRI transferred the patent rights to the new company along with Dr. X's services, rather than licensing the technology as it has done with other inventions.[20]

The Moonlighting Scientist

QUESTION: May a State scientist take a second job as a consultant to a company that funds research by the State? Does it matter whether the privately funded research is conducted for the State by the scientist or his agency? Does it matter if the scientist limits his private consulting services to projects unrelated to his State work?

ANSWER: Current State employees must avoid conflicts of interest and the appearance thereof in order to maintain public confidence in the integrity of official decisionmaking.

No State employee should have any interest, financial or otherwise, direct or indirect, or engage in any business or transaction or professional activity or incur any obligation of any nature, which is in substantial conflict with the proper discharge of the employee's duties in the public interest.[21] No State employee should: (1) accept other employment which will impair independent judgment in the exercise of official duties; (2) disclose confidential State information or use it to further personal interests; (3) use an official position to secure unwarranted privileges; (4) give reasonable basis for the impression that any person can improperly influence the employee or enjoy his or her official favor, or that the employee is affected by the kinship, rank, position or influence of any party or person; or (5) raise public suspicion that he or she is likely to be engaged in acts which violate the public trust.[22]

The Ethics Commission has considered these questions in the matter of "Dr. Y," a Research Scientist who headed a laboratory for the State Office of Mental Retardation and Developmental Disabilities (OMRDD). Dr. Y asked whether he could, as an outside activity, serve as a paid consultant to a pharmaceutical company that had invested funds for research at the same laboratory. Dr. Y conducted experiments in the OMRDD lab, supervised others, conducted collaborations with other labs, examined OMRDD lab budgets and reviewed the progress of OMRDD research; he submitted grant applications to private and governmental sources. The pharmaceutical company invested funds for a specific research project conducted both at the company lab and at Dr. Y's lab; scientists from each lab routinely exchanged data. Dr. Y offered to advise the company about the design and conduct of research to be conducted solely by the company, not jointly with OMRDD or the State.[23]

The Commission noted that Dr. Y proposed to be a paid consultant to a private for-profit company on matters unrelated to OMRDD's contract with company. The Commission noted that he would have a personal financial interest in maintaining good relations with the company which could affect his judgment in his official dealings with it. The public could perceive that his consulting arrangement would be in conflict with his duty of undivided loyalty to OMRDD. Dr. Y could not as a practical matter recuse himself from OMRDD duties in relation to the company. Because of the consultancy, the company might be perceived as having an unfair advantage when dealing with the State laboratory budget review committee of which Dr. Y was a member. The Commission concluded that there would be an appearance of a conflict of interest in violation of Public Officers Law § 74 if Dr. Y were to serve as a consultant to the company while it funded research at the laboratory he headed.[24]

Endnotes

1. *See* New York Pub. Off. Law § 74(2)(1999).
2. *See* N.Y. Comp. Codes R. & Regs. tit. 19 § 932.3(a)(1999).
3. *See* New York Pub. Off. Law § 73(2)(1999).
4. *See* Pub. Off. Law § 73(4).
5. *See* N.Y. Comp. Codes R. & Regs. tit. 19 § 932.
6. *See* N.Y. Comp. Codes R. & Regs. tit. 19 § 932.3(c).
7. *See* N.Y. Comp. Codes R. & Regs. tit. 19 § 932.3(e).
8. N.Y. Comp. Codes R. & Regs. tit. 19 § 932.3(d).
9. *See* N.Y. Comp. Codes R. & Regs. tit. 19 § 932.1(a).
10. *See* N.Y. Comp. Codes R. & Regs. tit. 19 § 932.5.
11. *See* Pub. Off. Law § 73-a(3)(1999).
12. *See* Pub. Off. Law § 73(8)(a)(i)(1999).
13. *See* Pub. Off. Law § 73(8)(a)(ii).
14. *See* Pub. Off. Law § 73(10).
15. *See* Pub. Off. Law § 73(8)(g).
16. *See* Pub. Off. Law § 73(8)(a)(ii).
17. *See* New York State Ethics Commission Advisory Op. No. 94-13.
18. *See* New York State Ethics Commission Advisory Op. No. 91-2.
19. *See* New York State Ethics Commission Advisory Op. No. 91-18.
20. *See* New York State Ethics Commission Advisory Op. No. 94-13.
21. *See* Pub. Off. Law § 74(2).
22. *See* Pub. Off. Law § 74(3)(a), (b), (c), (d), (f), (h).
23. *See* New York State Ethics Commission Advisory Op. No. 97-22.
24. *See id.*

Donald P. Berens, Jr., became Executive Director of the New York State Ethics Commission in 1999. He previously worked for three New York State Attorneys General, most recently as Deputy Attorney General for the Division of State Counsel. **The author gratefully acknowledges the assistance of Barbara Smith, Counsel to the New York State Ethics Commission, for reviewing this manuscript.**

NYSBA Attorneys in Public Service Committee is pleased to co-sponsor ABA Government and Public Sector Lawyers Division Events—July 2000

ABA Meets the Big Apple
2000 Annual Meeting Division Educational Events

New York City is host to the ABA's Annual Meeting, July 6-12, 2000. The Government and Public Sector Lawyers Division encourages New York State's public lawyers to attend Division events:

Friday, July 7
"Ethical Considerations in Public Sector Law"
Warwick Hotel, 65 W. 54th Street
2:00–5:00 p.m.

This program focuses on the unique ethical issues confronted by government and public sector lawyers. Topics examined include: scope of representation, public sector attorney-client privilege issues, duty to disclose lawyer misconduct and communication with represented persons. An entertaining interactive format using panelists who act out case scenarios encourages audience participation and involvement.

Saturday, July 8
"The 21st Century Public Lawyer: Problem Solver or Case Processor?"
Sheraton New York, 811 7th Avenue
2:00–5:00 p.m.

This interactive panel will bring together some of the country's leading practitioners and legal observers of the new "community oriented" approach to lawyering as well as professionals experienced in applying Alternative Dispute Resolution principles to community-level problems. It will examine the impact that a holistic, problem-solving approach is having on the profession, justice institutions, community and public safety, and their implications for future practice in public law offices.

Important Dates/Registration Info
Early Bird Registration—April 27, 2000
Housing Deadline—June 6, 2000
Advance Registration List Deadline—June 15, 2000

To register or for more information on housing, travel, theater tickets or programs, visit us at: http://www.abanet.org/annual/2000/home.html or call 312-988-5870.

NYSBA Committee on Attorneys in Public Service Co-Sponsored Event: October 14–18, 2000

The National Association of Administrative Law Judges' (**NAALJ**) Annual Meeting for 2000 will be held in Albany, NY (Albany 2000 or **A2K**) and is being co-sponsored by the New York State Administrative Law Judges Association (**NYSALJA**), the Government Law Center of Albany Law School (**GLC of ALS**) and the New York State Bar Association (**NYSBA**), **Committee on Attorneys in Public Service**.

The conference theme of "**Administrative Law in the New Millennium**, ***Challenges and Opportunities"*** will surely pique the interests and attention of all attendees. Take advantage of the excellent schedule of educational and social events, network, and make connections with exhibitors. Mark your calendars today.

The conference begins on **Saturday, October 14th** and ends on **Wednesday, October 18th, 2000**.

(MCLE Accredited) Educational Events to include:

Judicial Ethics and Independence • Security Issues for Judges • Agency and Judicial Review of Administrative Decisions • Computer Basics and Advanced Uses • New York Adjudication • Workers Compensation • Technology in Administrative Review • The Peer Review Process in Administrative Adjudication • Evidence: Scientific Evidence and Expert Evidence in Administrative Hearings • Complex Litigation • Environmental Justice and Associated Issues • Writing • Administrative Issues • Making Credibility Determinations • Alternative Dispute Resolution in Administrative Proceedings

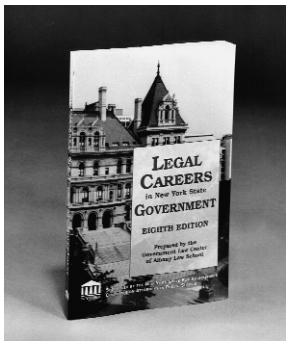
ACCOMMODATIONS: Desmond Hotel, Albany, NY

REGISTRATION: For more information, visit www.NAALJ.com or contact: Administrative Law Judge Marc P. Zylberberg at 518-402-0748.

Conference Chair—Tyrone T. Butler, Chief Administrative Law Judge
NYS Department of Health

Legal Careers in New York State Government—Eighth Edition

NEW RELEASE!



Editors

Patricia E. Salkin, Esq.
Director of the Government Law Center of Albany Law School

Michele A. Monforte
Program Associate for the Government Law Center

Prepared by the Government Law Center of Albany Law School

This unique publication was compiled to assist law students and lawyers who are considering careers and/or work experience in public service with the State of New York. It has been expanded to include comprehensive information on employment opportunities with the government in New York State. Part I is an overview of the types of jobs and internships available. The next three sections cover employment with state agencies, opportunities with the state legislature, and employment with municipal governments, public defender's offices and district attorney's offices.

In addition to descriptions of the various agencies' functions, the book offers practical tips on how to secure employment with the executive and legislative branches of state government, as well as current addresses for government employers.

1999 • 234 pp., softbound • PN: 41299
List Price: $50 (incls. $3.70 tax)
Mmbr. Price: $35 (incls. $2.59 tax)

Sponsored by the New York State Bar Association's Committee on Attorneys in Public Service.

To order

Call 1-800-582-2452
Source code: cl1097
(05/00)

New York State Bar Association

PUBLICATIONS to help you!

Criminal Practice

Authors
Hon. Leslie Crocker Snyder
Alex Calabrese, Esq.
Bonnie R. Cohen-Gallett, Esq.

Criminal Practice is a practical guide for attorneys representing clients charged with violations, misdemeanors or felonies.

1998, 206 pp., softbound,
PN: 4064
Non-member Price: $60
Member Price: $50

New York Criminal Practice
Second Edition

Editor
Lawrence N. Gray, Esq.

Editor-in-chief Lawrence Gray and 28 contributors consisting of prominent full-time practitioners, judges, prosecutors and public defenders have put considerable effort into producing what should prove to be the leading criminal practice reference in New York State.

1998, 892 pp., hardbound,
PN: 4146
Non-member Price: $130
Member Price: $110

New York Municipal Formbook
Second Edition

Author
Herbert A. Kline, Esq.

Editor
Nancy E. Kline, Esq.

The *Municipal Formbook* contains over 500 forms, edited for use by town, village and city attorneys and officials.

1999, 1650 pp., loose-leaf,
2 volume, PN: 41608
Non-member Price: $140
Member Price: $120
With Diskette:
Non-member Price: $190
Member Price: $170

Public Sector Labor and Employment Law
Second Edition

Editors
Jerome Lefkowitz, Esq.
Melvin H. Osterman, Esq.
Rosemary A. Townley, Esq., Ph.D.

This landmark text is the leading reference on public sector labor and employment law in New York State.

1998, 1304 pp., hardbound,
PN: 4206
Non-member Price: $140
Member Price: $115

Representing People with Disabilities
Second Edition

Editor
Peter Danziger, Esq.

This newly organized and updated second edition of *Representing People*

with Disabilities is a comprehensive reference encompassing the myriad legal concerns of people with disabilities including an in-depth examination of the Americans with Disabilities Act.

1997, 794 pp., loose-leaf,
PN: 42157
Non-member Price: $120
Member Price: $90

Zoning and Land Use

Authors
Michael E. Cusack, Esq.
John P. Stockli, Jr., Esq.

This publication is devoted to practitioners who need to understand the general goals, framework and statutes relevant to zoning and land use law in New York State for intermittent purposes.

1998, 106 pp., softbound,
PN: 4239
Non-member Price: $65
Member Price: $55

Zoning Board of Appeals Practice in New York

Authors
Robert J. Flynn, Esq.
Robert J. Flynn, Jr., Esq.

Zoning Board of Appeals Practice in New York is an invaluable reference to assist the practitioner in preparing a proper record.

1996, 210 pp.,
PN: 4240
Non-member Price: $60
Member Price: $45

NYSBA CLE Publications can be Purchased Online.
You can purchase a subscription to CLE publications online—over twenty-five titles are now available on the Internet, and the complete reference library will be added in the near future. Your subscription includes unlimited access to CLE reference material. CLE publications on the Internet are linked—**at no extra charge**—to the cases and statutes cited.

For information call 800.364.2512
Access our site at: www.nysba.org

NEW!! "MCLE Take-Out" Resources Especially for Government and Non-Profit Attorneys

The NYSBA is pleased to present audio and video tapes to enable you to earn MCLE credits* on your own schedule! In addition to NYSBA's other offerings, we are pleased to make these tapes from the 1999 and 2000 Annual Meeting and Spring CLE programs available to you.

Ethics for Government Attorneys

Earn 3 New York MCLE credits in "ethics and professionalism" by viewing or listening to this recording of the January 1999 Annual Meeting presentation. These tapes (available in either audio or video) offer a very practical guide to the various ethical issues facing attorneys in public service. Written materials accompany the recordings.

1999
PN: 3871 (video album); 2871 (audio album)

NYSBA Member Prices:
Video Album: $100;
Audio Album: $80

Non-NYSBA Member Prices:
Video Album: $150;
Audio Album: $135

Available in late Spring 2000:

Is the Supreme Court Changing the Balance of Power? The Sovereign Immunity Cases

Earn 3 MCLE credits in "professional practice/practice management" by listening to this recording of the January 2000 Annual Meeting presentation. USC Law School Professor Erwin Chemerinsky, a nationally renowned expert on the topic of sovereign immunity, spoke on when state government and state officers can be sued in federal and state courts. It also covered the recent and pending Supreme Court cases, as well as provided a thorough coverage of the law in this area. This audio program is accompanied by written materials.

Administrative Adjudication—A Comprehensive View

Adjudication in the administrative forum is a relatively unknown specialty area of practice. This program focused on aspects of practice in the administrative forum, including presentations on evidentiary rules in administrative forums, the art of judging in hearings, case presentations, Article 78 discussions and more. This program will be available in audio format and will be accompanied by written materials.

IMPORTANT NOTE: Buy one video or audio album and multiple copies of the course materials for group use. Each member of the group may earn MCLE credit—call our CLE Registrar for more details.

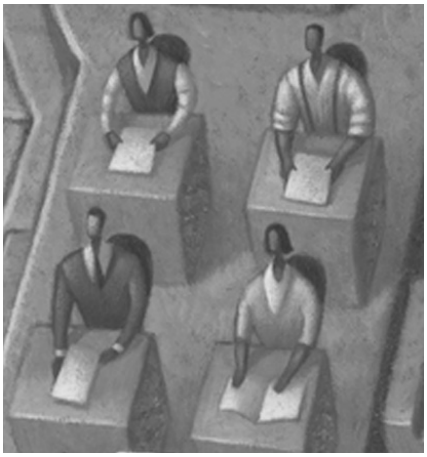
*Only attorneys in practice for more than two years can earn MCLE credits through the use of tapes.

To Order by Mail, send a check or money order to: CLE Registrar's Office, N.Y.S. Bar Association, One Elk St., Albany, NY 12207*

*Please specify shipping address (no P.O. box) and telephone number

To Order by Telephone, call **1-800-582-2452** (Albany & surrounding areas 518-463-3724) and charge your order to American Express, Discover, MasterCard or Visa. Be certain to specify the title and product number.

Source Code: CL1098 (5/00)



NEW YORK STATE BAR ASSOCIATION

ATTORNEYS IN PUBLIC SERVICE

Subcommittees:

Education

Administrative Law Judges

Non-Profit Attorneys

Awards

Court Attorneys

Technology

Section Liaisons

Legislation and Policy Review

Get Involved serve on a COMMITTEE

☐ Yes, I would like to volunteer for an **Attorneys in Public Service** subcommittee. **(You must be a NYSBA member to serve on a subcommittee).**

☐ Education
☐ Administrative Law Judges
☐ Non-Profit Attorneys
☐ Awards
☐ Court Attorneys
☐ Technology
☐ Section Liaisons
☐ Legislation and Policy Review

☐ I am not a NYSBA member. Please send information.

Please Print

NAME

OFFICE NAME

ADDRESS

CITY STATE ZIP

PHONE FAX

E-MAIL

I suggest the committee consider the following activities:

_____

_____

_____

_____

_____

Please copy this form and return to Membership Office. FAX 518.487.5579

New York State Bar Association
Membership Department
One Elk Street, Albany NY 12207
Phone 518.487.5577
E-mail: membership@nysba.org
http://www.nysba.org

NYSBA Membership Application

☐ Yes, I want to join the New York State Bar Association.

Name _____

Address _____

_____

City _____ State _____ Zip _____

Office phone ( ) _____

Home phone ( ) _____ Fax number ( ) _____

Date of birth ____/____/____ E-mail address _____

Law school _____ Graduation date _____

States and dates of admission to Bar: _____

_____

Join Today —
It Pays to Be a Member

NYSBA membership will:

- help you earn **MCLE credits** — anywhere and anytime;
- allow you access to outstanding **personal and professional development** resources;
- keep you updated on **current legal issues** in New York law;
- help you to become part of a growing nationwide **network** of legal professionals;
- enable you to have an **impact** on the profession;
- link you to a number of money and time saving **technology resources.**

ANNUAL MEMBERSHIP DUES (Check One)

Class based on first year of admission to bar of any state.

REGULAR MEMBER

☐ Attorneys admitted 1992 and prior	$ 235.
☐ Attorneys admitted 1993-1994	155.
☐ Attorneys admitted 1995-1996	100.
☐ Attorneys admitted 1997-1999	70.
☐ Newly admitted attorneys	FREE
☐ Law students / graduated students awaiting admission	10.

NON-RESIDENT MEMBER

Out of state attorneys who do not work in New York

☐ Attorneys admitted 1995 and prior	95.
☐ Attorneys admitted 1996-1999	70.

☐ **Send Information on the Dues Waiver Program**

DUES PAYMENT

☐ Check *(payable in U.S. dollars)*

☐ MasterCard

☐ Visa

☐ American Express

☐ Discover

Account No.

Expiration Date _____ Date _____

Signature _____

TOTAL ENCLOSED $ _____

Please return this application to:

Membership Department
New York State Bar Association
One Elk Street
Albany NY 12207

Phone 518.487.5577
FAX 518.487.5579
E-mail: membership@nysba.org
http://www.nysba.org