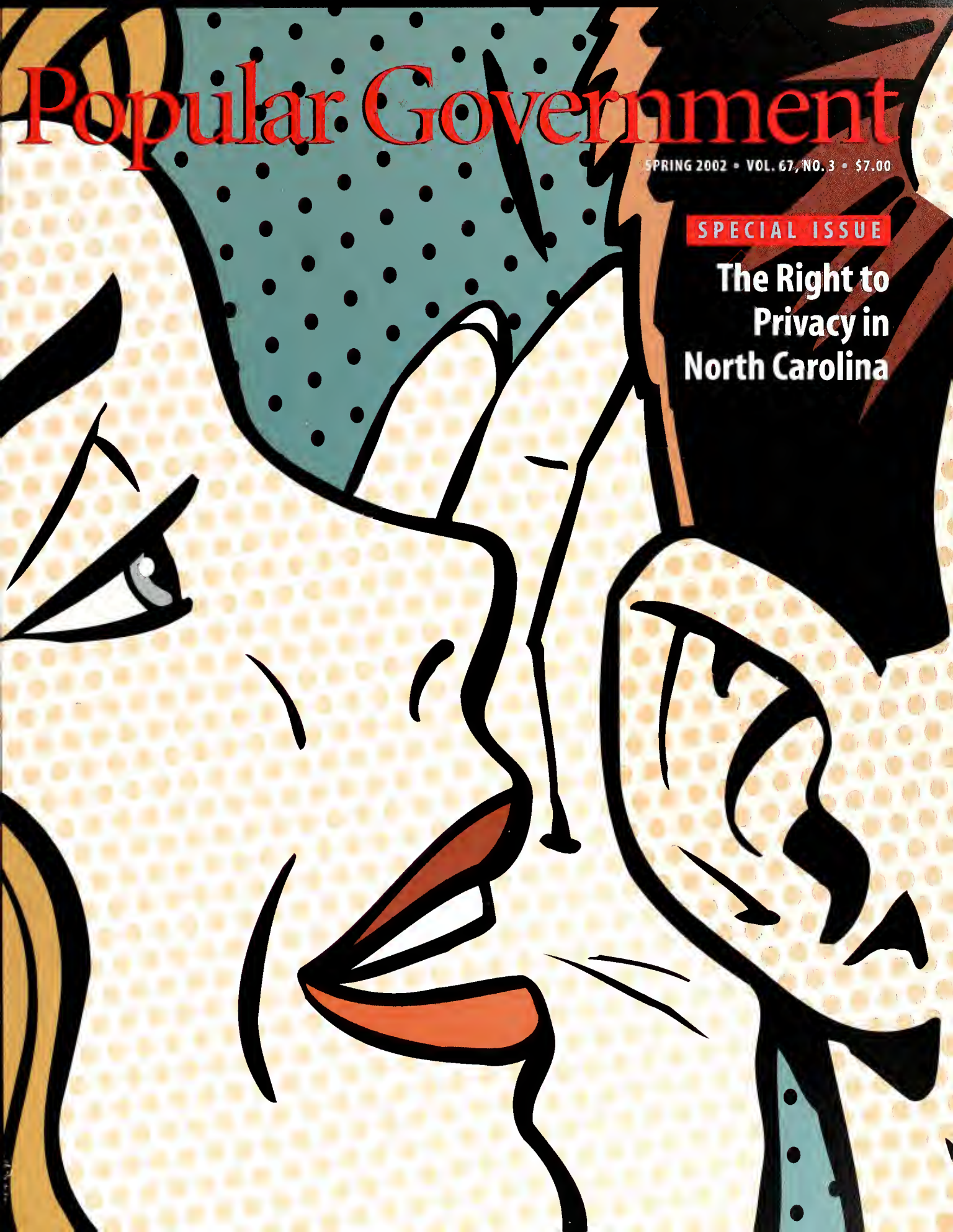
PUBLISHED BY THE INSTITUTE OF GOVERNMENT ■ THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL

Popular Government

SPRING 2002 • VOL. 67, NO. 3 • $7.00

SPECIAL ISSUE

The Right to Privacy in North Carolina



Popular Government

James Madison and other leaders in the American Revolution employed the term "popular government" to signify the ideal of a democratic, or "popular," government—a government, as Abraham Lincoln later put it, of the people, by the people, and for the people. In that spirit *Popular Government* offers research and analysis on state and local government in North Carolina and other issues of public concern. For, as Madison said, "A people who mean to be their own governors must arm themselves with the power which knowledge gives."

POPULAR GOVERNMENT (ISSN 0032-4515) is published four times a year (summer, fall, winter, spring) by the Institute of Government. Address: CB# 3330 Knapp Building, UNC-CH, Chapel Hill, NC 27599-3330; telephone: (919) 966-5381; fax: (919) 962-0654; Web site: http://iog.unc.edu/. Subscription: $20.00 per year + 6.5% tax for NC residents. Second-class postage paid at Chapel Hill, NC, and additional mailing offices.

POSTMASTER: Please send changes of address to Eva Womble, Institute of Government, CB# 3330 Knapp Building, UNC-CH, Chapel Hill, NC 27599-3330; telephone: (919) 966-4156; fax: (919) 962-2707; e-mail: womble@iogmail.iog.unc.edu.

Established in 1931, the Institute of Government provides training, advisory, and research services to public officials and others interested in the operation of state and local government in North Carolina. The Institute and the university's Master of Public Administration Program are the core activities of the School of Government at The University of North Carolina at Chapel Hill.

Each year approximately 14,000 city, county, and state officials attend one or more of the 230 classes, seminars, and conferences offered by the Institute. Faculty members annually publish up to fifty books, bulletins, and other reference works related to state and local government. Each day that the General Assembly is in session, the Institute's *Daily Bulletin*, available in print and electronically, reports on the day's activities for members of the legislature and others who need to follow the course of legislation. An extensive Web site (http://iog.unc.edu/) provides access to publications and faculty research, course listings, program and service information, and links to other useful sites related to government.

Support for the Institute's operations comes from various sources, including state appropriations, local government membership dues, private contributions, publication sales, and service contracts. For more information about the Institute, visit the Web site or call (919) 966-5381.

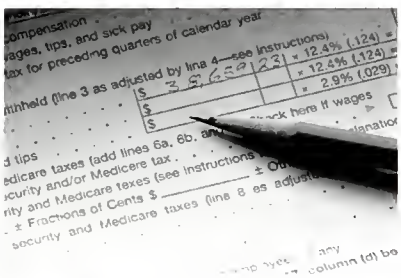
Popular Government

Spring 2002 • Volume 67, Number 3

Page 6

Gary Allen / News & Observer

Page 13



Page 20

Page 36

ON THE COVER

In today's technologically advanced, interconnected world, people are increasingly concerned about maintaining some degree of privacy. Recent developments have intensified the debate about the proper balance between privacy and other societal interests, such as public safety and health.

FEATURE ARTICLES

DEPARTMENTS

New Environmental Finance Center Focuses on Real-World Issues

ANN C. SIMPSON

UNC–Chapel Hill's School of Government, in conjunction with the Kenan Center for Private Enterprise, has a new research and assistance center focusing on the real-world problems of environmental finance and management. The Environmental Finance Center at the University of North Carolina, called the efc@unc for short, aims to "provide a bridge between students and faculty in the university who work principally on environmental financing, management and planning tools and the governments and businesses whose job it is to use those tools for the public interest," according to its mission statement.

"Local governments have a diverse set of challenges in the environmental area," explains Richard Whisnant, director of the center and a faculty member in environmental law at the School of Government. "Among them are providing safe drinking water, handling and treating wastewater, collecting and disposing of solid wastes, and minimizing the many adverse effects of growth and development."

The common denominator of these and all other environmental governance challenges, Whisnant says, is that they have costs—and finding the financing to pay these costs is not always as simple as getting a federal grant. "Finance has become a critical, sometimes complicated, requirement of improved environmental management," he observes.

Started with a planning grant from the U.S. Environmental Protection Agency in 1998, the efc@unc has blossomed into an ongoing center with research and assistance projects in a wide variety of environmental areas (see sidebar, opposite). Whisnant and Jeff Hughes, associate director and an international consultant on environmental finance (as well as a former utilities director in Chatham County), are the principal staff. Other faculty members and students work with them on projects.

In addition to its project work, the center is developing partnerships with a wide range of organizations that provide training and assistance to environmental leaders in local government. It also has joined eight other environmental finance centers at universities around the United States to create a network of people working on environmental finance and management problems within academic settings but with a mission to help with real-world issues.

Additional information is available at the center's Web site, www.efc.unc.edu. To learn more about the center's work or to offer suggestions for projects or research that should be undertaken, contact Whisnant at (919) 962-9320 or richard_whisnant@unc.edu, or Hughes at (919) 843-4956 or jhughes@unc.edu.

efc@unc projects

During 2001 the efc@unc

- published a major report on the costs and financing of North Carolina's Million Acres land-conservation initiative;
- began work with several other environmental finance centers on a national pilot project on source-water protection, which is based in Rutherford County; and
- delivered a comprehensive environmental finance curriculum to the U.S. Environmental Protection Agency and other environmental finance centers around the country.

For 2002 the efc@unc has been awarded a grant to develop innovative distance-education modules on environmental finance topics for engineering master's degree students and local government environmental professionals who have had little opportunity for practical environmental finance training. This project is the start of long-term efforts that are central to the strategic plan of the efc@unc: to use information technology as a bridge between environmental finance expertise and government officials (and their consultants and contractors) who most directly need that expertise.

Another of the center's efforts in this regard is a database of state-based environmental financing sources in the Southeast. The database will include grant and loan sources that are funded by state or local governments or other entities that operate primarily within a state or a similar limited geographical area.

Consortium Builds Bridges Between Government and Youth

The North Carolina Civic Education Consortium, a program of the Institute of Government, has received major grants for several initiatives to help local governments involve young people in issues and programs that concern them and their communities:

- A pilot project funded by the Golden LEAF Foundation will develop youth leadership programs in two rural counties, Bertie and Swain. Initially the consortium will organize model youth councils linked to local governments and create cross-generational teams to explore the economic development challenges facing these counties. In the second phase of the project, the consortium will help other rural communities replicate the most successful elements of the pilot program.

Leslie Anderson, North Carolina Civic Education Consortium

Already the grant has allowed Bertie County to hire a youth coordinator to develop a youth council and build a network of programs that serve or involve young people.

- With a grant channeled through Providence College (in Rhode Island) from funds from the Pew Charitable Trusts, the consortium will develop a network of twenty-four high schools across the state, then work with a team of students at each school to inventory civic involvement opportunities. The teams will lead focus groups of parents, students, teachers, and others to identify these opportunities and to select at least one strategy for their high school to use to improve youth civic involvement. Local governments and school boards will be partners in this effort.
- A Small Grants Program funded by the Z. Smith Reynolds Foundation will provide $1,000 to $10,000 to outstanding youth involvement programs. The consortium encourages local governments, including school boards, to apply for these grants. Applications for 2002 grants will be available from the consortium office by July 1, 2002. Recipients will be selected by December 1, 2002.
- The consortium also has received a substantial two-year grant from the Carnegie Corporation of New York to enhance its organizational capacity, including fund development and strategic planning. By improving its internal practices, the consortium will increase its ability to support and expand its most successful programs.

Research shows that giving young people a chance to participate in government decision making is the most effective form of civic education, according to consortium director Debra Henzey. "It fosters lifelong civic interest and involvement."

The consortium's work builds on a tradition going back to the 1940s, when Institute of Government founder Albert Coates involved the Institute in civic education classes for teachers and young people. The original efforts died out during World War II, but local government officials asked the Institute to restore this part of its mission during a long-term planning process in the mid-1990s. Government leaders were increasingly concerned that the quality of public debate on important issues had declined and that fewer people in communities were willing or prepared to assume leadership roles.

The consortium was founded in 1997 with support from the Z. Smith Reynolds Foundation. Enlisting as a partner is free. For more information on the consortium's programs or to send information about local government youth programs, contact Henzey at (919) 962-8273 or henzey@iogmail.iog.unc.edu.

Teleconference Provides Timely, Economical Look at Changes in Law

On December 6, 2001, the North Carolina General Assembly ratified Senate Bill 914, making significant changes in the laws governing public building construction. Most of these changes became effective on January 1, 2002, creating an immediate need for local and state government officials to comply.

The Institute of Government met this need by collaborating with other groups involved in public construction to organize a statewide teleconference, which aired on February 20, 2002, to an estimated 800 viewers. According to Frayda Bluestein, associate professor of public law and government at the Institute and a principal organizer of the conference, the audience's response suggests that the program was successful on many fronts. "It's an example of how we can use technology to communicate useful and timely information at minimal cost," Bluestein said.

The teleconference reached a broad range of people, including local and state government officials, private-sector architects and engineers who work on public projects, and even some construction contractors. Viewers got the technical information they needed in a timely manner. They learned, for example, the new dollar thresholds that trigger the competitive-bidding requirements in public construction and the new requirements for dispute resolution and minority participation.

By broadcasting to enough sites statewide, organizers sought to ensure that no person had to travel more than 100 miles to view the program. Approximately twenty sites, mostly community colleges and university campuses, hosted the program. Other viewers accessed the program through Web streaming technology, which allowed them to view it on a personal computer.

With the financial support of the North Carolina Department of Administration, the program was offered at no cost to those attending. Other organizations providing input and in-kind support included The University of North Carolina, the Community Colleges System, the North Carolina School Boards Association, the North Carolina Hospitals Association, the North Carolina League of Municipalities, and the Association of County Commissioners. The program was produced by the Agency for Public Telecommunications, which is a part of the N.C. Department of Administration.

Most sites had telephone, e-mail, and fax connections with the studio. Breaks were scheduled so that questions from the sites could be received and then answered during two panel discussions included in the teleconference. Behind the scenes, experts representing various agencies screened questions to avoid duplication and to make sure that the panel addressed issues of broad interest to the audience.

Materials for the program were made available in advance on a Web site created especially for the program. In most cases, those attending were able to print out the materials.

For information about the substance of the new law, visit http://ncinfo.iog.unc.edu/pubs/nclegis/nclegis2001/pdfs/Ch21web.pdf or contact Bluestein at bluestein@iogmail.iog.unc.edu. Videos of the conference are available for checkout from the Institute of Government library. Teleconference materials, which include a complete summary of the new legislation, are available at the teleconference Web address: http://ncinfo.iog.unc.edu/faculty/bluestein/senatebill914/.

"Being able to view the program at the office instead of traveling is a wonderful opportunity."

— Participant

North Carolina Agency for Public Telecommunications

New Scholarships Available for Institute Classes

The Local Government Federal Credit Union (LGFCU) is offering its members the opportunity to apply for scholarships that will cover tuition for Institute of Government classes, conferences, and seminars. Scholarships will be awarded quarterly. Application deadlines are March 15, June 15, September 15, and December 15. Funds are limited, so applications should be sent in as early as possible each quarter.

For more information and an application form, call (800) 344-4846 or e-mail Info@LGFCU.org. LGFCU plans to put information about the scholarship program on its Web site (www.LGFCU.org) in the near future.

MPA Students Present Results of Practical Research

How much Medicaid and State Children's Health Insurance Plan funding did North Carolina lose because Hispanics were undercounted in the 2000 census?

Which community-based programs for delinquent juveniles are most likely to help young people avoid further trouble with the law?

What lessons can be learned from Wake County's solution to local school financing disputes?

These and similar questions are answered in this year's "capstone" papers — reports of practical research conducted each year by students graduating from the Master of Public Administration (MPA) Program at UNC–Chapel Hill.

Each MPA student distills his or her capstone project into a five-page summary and presents the findings at the MPA Program's annual Practical Research for Public Officials Conference, held this year on April 19, 2002. The conference is open to the public, and the topics of all the papers are listed on the MPA Web site: www.iog.nc.edu/uncmpa/students/capstone.html.

For information about the conference or to order papers, contact Jessica Russell at (919) 962-0425 or mpastaff@iogmail.iog.unc.edu.

Listservs Connect Local Governments

The Institute of Government offers a number of listservs that allow local government personnel to share information with their peers and Institute faculty. According to Philip Young, who manages the program, "The lists are wonderful resources for connecting with others doing similar work and for learning about the latest local government issues that a group is facing. All it takes for an individual to use a list is a computer with an Internet connection and an e-mail account."

Listservs collect multiple e-mail addresses under a single e-mail address and allow members to send a message to everyone on the list using that single address—for example, listservname@listserv.unc.edu.

To join a list or to get more information about how listservs work, contact Young at (919) 962-0592 or pyoung@imap.unc.edu.

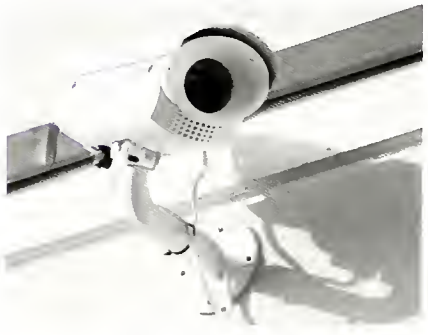
List Name	Group Served	Administrator
buslic	Business Licensing	Philip Young
ccmanagers	City and County Managers	William Rivenbark
cclub	Candidate's Club for Tax Assessors and Administrators	Joseph Hunt
clerks	City and County Clerks	Fleming Bell
dssattorneylist	Department of Social Services Attorneys	Janet Mason and John Saxon
humanresources	Human Resources and Personnel	Diane Juffras
fodg	Facilitation and Organizational Development Group	John Stephens
iogcriminal	Recent North Carolina Criminal Court Decisions	Robert Farb
instofgovpubs	News of Institute of Government Recent Publication Releases	Katrina Hunt
lglaw	Local Government Lawyers	Fleming Bell
ncard	Registers of Deeds	Philip Young
ncfinance	Finance Officers and Directors	Gregory Allison
ncgis	Geographic Information Systems	Philip Young
nclgisa	Local Government Information Systems Associations	Philip Young
nclgba	Local Government Budget Association	Maureen Berner
ncplan	Planners and Planning Departments	David Owens
ncpma	Property Mappers Association	David Owens
ncpublicworks	Public Works	Richard Whisnant
ncpurchasing	Purchasing Agents	Frayda Bluestein
soilconservation	Soil Conservation and Management	Richard Whisnant
ptax	Property Tax Assessors and Administrators	Joseph Hunt
waste	Waste Management	Richard Whisnant

On June 11, 2001, the U.S. Supreme Court ruled that police violated the Constitution's prohibition against unreasonable searches when they used a thermal imager (which monitors heat patterns emanating from the walls of a house) without a search warrant. The decision reversed a lower court's ruling that the homeowner had no reasonable expectation of privacy in the heat emitted from the walls of his home by the lights he used to grow marijuana in his garage.

NC Division of Tourism, Film and Sports Development

After Dale Earnhardt's fatal car crash during the Daytona 500 on February 18, 2001, his widow argued that public disclosure of the medical examiner's autopsy photographs would violate the family's right to privacy. The Florida legislature responded by amending the state's public records law to bar the release of autopsy records without a court order.

In January 2001, surveillance cameras photographed 100,000 spectators as they passed through the turnstiles at the Super Bowl in Tampa, Florida. A biometric face-recognition system then matched the photographs against a database of convicted criminals maintained by the FBI and state and local police. Critics argued that the system violated individual privacy. Advocates responded that it was no more intrusive than the routine video surveillance that most people encounter every day in banks, stores, malls, and office buildings, at ATM machines, and on public streets.



Privacy and the Law

John L. Saxon

More than 80 percent of Americans say that they are concerned about the loss of their personal privacy— especially about the collection, use, and disclosure of personal, financial, and medical information by government agencies, insurance companies, banks, employers, medical providers, on-line businesses, and private data-collection agencies.[1]

The exponential growth of information technology—computerized systems of data collection, storage, and retrieval, electronic surveillance devices, and so forth—during the past thirty years has contributed to public concern about privacy by making it easier and easier for government agencies, businesses, and individuals to gather and exchange information.[2]

Concern about privacy is not new, however. More than one hundred years ago, responding to what they viewed as the unprecedented invasion of the "sacred precincts of private . . . life," Samuel Warren and Louis Brandeis asserted in the *Harvard Law Review* that the law should protect the "privacy of private life" by recognizing individuals' rights to prevent others' access to, use of, and public disclosure of their personal writings, thoughts, feelings, likeness, or private acts.[3] In the 1960s many people, including Justice William O. Douglas, believed that government surveillance constituted the primary threat to privacy.[4] Today many people think that the private sector threatens privacy as much as, or more than, government does.[5]

What Is Privacy?

Although privacy is clearly an important legal and social concept, only recently have there been any serious efforts to analyze what "privacy" means.[6] In one sense, privacy is a *nonlegal* concept, with psychological, social, and political dimensions, that describes the boundaries between an individual and other people, society, and government—between matters, beliefs, communications, and activities that are personal or private in nature and those that are social in nature or of public concern.[7] Privacy also is a *legal* concept, consisting of moral rules, social norms, and legal rights that recognize, protect, and sometimes limit individuals' expectations and claims.

In 1880, Judge Thomas Cooley offered one of the first definitions of the right to privacy: the right "to be let alone."[8] Cooley's definition was subse-

The author is an Institute of Government faculty member who specializes in social services, elder law, and child support issues. Contact him at saxon@iogmail.iog.unc.edu.

quently adopted and made famous as "the right most valued by civilized men" by Justice Brandeis in his 1928 dissent in *Olmstead v. United States*.[9]

More recently, privacy has been defined as

- the right to control others' access to, use of, and disclosure of information about oneself;[10]
- the right to be free from unjustified public scrutiny; and
- the right to be free from unreasonable intrusions on one's solitude and repose.

In addition, privacy today is generally understood to include both

- the right to be free from unwarranted surveillance or searches of one's home, person, or communications by government agencies, and
- the right to be free from governmental control, regulation, or coercion with respect to personal decisions or matters that lie at the core of individual autonomy (such as sexuality, birth control, abortion, family relationships, and personal beliefs).

No single definition of privacy, however, is wholly satisfactory or complete.[11] Instead, "privacy" appears to be an umbrella term that encompasses a wide variety of interests, claims, and rights.[12]

Why Does the Law Protect Privacy?

Every person has some degree of personal privacy regardless of whether the law recognizes and protects it. An individual, however, has a legal right to privacy only to the extent that the law (1) recognizes as legitimate that individual's interest, expectation, or claim to privacy; (2) imposes a corresponding duty on others not to invade or interfere with the individual's privacy; and (3) protects his or her right to privacy against others.[13]

But why should the law protect individual privacy? What individual and social interests does privacy serve?

Every individual has an interest in personal privacy, solitude, and autonomy. Simply put, some matters are "nobody else's business."[14] Sociologist Amitai Etzioni argues that privacy is a veil behind which one may shield what is legitimately private from public view.[15] (Richard Posner offers a contrary view, which may not be widely shared: that privacy facilitates fraud and misrepresentation by allowing people to conceal true but embarrassing information about themselves from others in order to gain unfair social or economic advantage.)[16]

Psychologically and socially, people need a certain degree of privacy and solitude—"a refuge within which [they] can shape and carry on [their] lives . . . without the threat of scrutiny, embarrassment, judgment, and the deleterious consequences they might bring."[17] Privacy protects individual autonomy; safeguards people from tangible social or economic harm or discrimination resulting from the disclosure of sensitive, embarrassing, or negative information;[18] and allows people to establish and maintain important personal, social, and professional relationships.[19]

Privacy is more than an *individual* value, however; it also is a social one. Privacy is

> *important not only because of its protection of the individual as an individual but also because individuals share common perceptions about the importance and meaning of privacy, because it serves as a restraint on how organizations use their power, and because privacy—or lack of privacy—is built into systems and organizational practices and procedures . . . [thereby giving] privacy broader social, not only individual, significance.*[20]

Moreover, in at least some instances, privacy serves public or social purposes that are unrelated to, or go beyond, the protection of individuals' interests. For example, federal rules regarding the confidentiality of treatment records for alcohol and drug abuse protect patients from stigma or harm they might suffer as a result of public disclosure of their status. But the rules also serve an important public and social purpose: minimizing the social impact of alcohol and drug use by encouraging patients to seek treatment without fear of public scrutiny and by protecting the confidential relationship between patients and professionals that is required for successful treatment.[21]

Is Privacy Absolute?

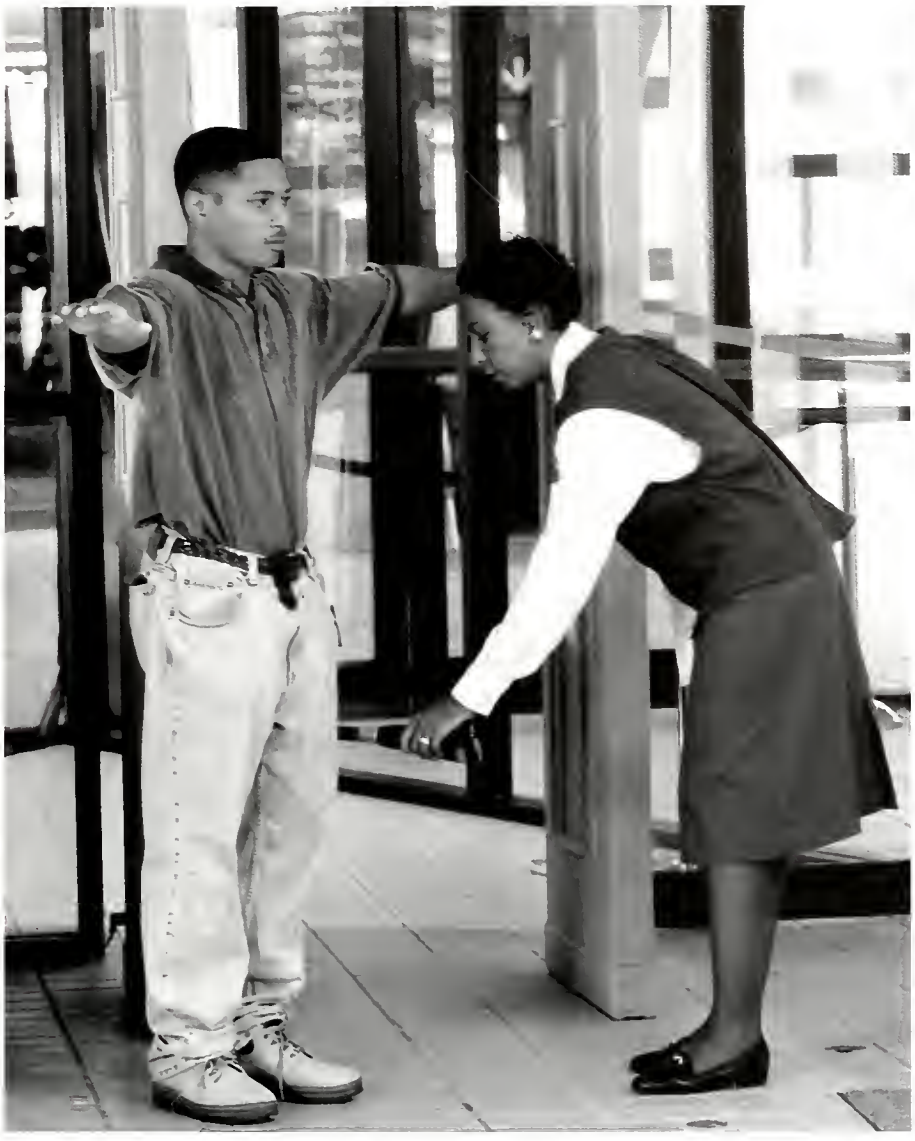
Is privacy absolute? The short answer is no.

The reason is threefold. First, absolute privacy is simply impossible in society. The very act of engaging in personal relationships with others and living in society necessarily requires an individual to relinquish his or her personal privacy to some extent.[22]

Privacy protects individual autonomy; safeguards people from tangible social or economic harm or discrimination resulting from the disclosure of sensitive, embarrassing, or negative information; and allows people to establish and maintain important personal, social, and professional relationships.

Second, legal rights to privacy are more limited in scope than the concept of privacy itself. Privacy encompasses a broad range of individual and social interests, and not every invasion or loss of privacy is of sufficient importance or weight to warrant legal protection.[23]

Third, and most important, although privacy is an important individual and social value, it is not the only value that the law and public policy must take into consideration.[24] Individual and social interests in privacy often must be balanced against competing individual and social interests, such as governmental account-



ability, public safety, and administrative efficiency.[25] In some instances the competing interests may either limit or completely override individual and social interests in privacy. For instance, virtually every statute or legal rule recognizing an individual's legal right to privacy in the information gathered about him or her includes one or more exceptions under which otherwise private, privileged, or confidential information may or must be disclosed to someone in some circumstances for some purpose.[26]

The real issue, of course, is how much weight to give privacy versus other interests in any particular situation. Some privacy advocates contend that a presumption of privacy should be the "default setting of the Information Age."[27] By contrast, sociologist Amitai Etzioni argues that privacy should not be accorded special status. Instead, it should be treated like any other individual right that must be balanced with concerns for the common good.[28]

What Rights to Privacy Does the Law Protect?

It is generally agreed that the law recognizes and protects four distinct rights to privacy:

- Freedom from unreasonable searches by government agencies or officials
- Individual autonomy—the right to make personal decisions about sexuality, birth control, abortion, and family relationships free from governmental control or coercion
- Freedom from unwarranted intrusions on personal solitude or seclusion
- "Informational privacy," protecting individuals from unreasonable collection, use, and disclosure of personal information

Each of these rights depends on dozens (if not hundreds) of laws—federal and state constitutional provisions, federal and state statutes and regulations, court decisions, and the common law.[29] Those laws determine what privacy means in particular situations: whether an individual has a legal right to privacy, what the nature and the scope of that right are, and how that right will be protected.[30]

Constitutional Rights

Although the U.S. Constitution does not expressly refer to a right to privacy, it clearly protects at least three aspects of individual privacy. First, the Fourth Amendment's prohibition against unreasonable searches limits government surveillance that unduly intrudes on an individual's home, person, or communications.[31] (For a detailed discussion of the Fourth Amendment's guarantees, see the article on page 13.)

Second, the Supreme Court has recognized a constitutional right of privacy that protects individual liberty and autonomy by limiting government interference with or control of personal decisions regarding birth control, abortion, marriage, parenting, and family.[32]

Third, the Supreme Court's 1977 decision in *Whalen v. Roe* suggested that the Constitution's protection of individual privacy encompasses a right to "informational privacy," which may limit the authority of federal, state, and local governments to obtain, use, or disclose personal information about individuals. The *Whalen* case involved a New York law that required doctors to send a copy of all prescriptions for certain legal but dangerous drugs to the state health agency, which maintained a computerized database including the name, the address, and the age of the patients for whom the drugs were prescribed. The Court recognized that "the accumulation of vast amounts of personal information in computerized data banks or other massive government files" threatens individual privacy.[33] However, the Court also recognized that the government's collection and use of personal informa-

Several municipalities in North Carolina are authorized to mount cameras at intersections to photograph drivers running red lights.

RANDY JAY HARRINGTON

tion is necessary in order to collect taxes, enforce criminal laws, protect the public health, and administer government programs, and that its right to collect personal information generally is accompanied by a corresponding legal duty to avoid unwarranted disclosure or use of that information.

Further, the *Whalen* decision recognized, at least implicitly, that the Constitution establishes a floor for the protection of individual privacy, including a right in some circumstances not to have one's private affairs made public by the government. However, the Court held that New York did not violate the constitutional privacy rights of patients because the state's collection of prescription records from pharmacists was reasonably related to its legitimate interest in controlling the distribution of dangerous drugs and minimizing their misuse, and the law adequately protected the patients' confidentiality by limiting access to, use of, and disclosure of the information.

Although the North Carolina Constitution does not expressly recognize a right to informational privacy, both the North Carolina Supreme Court and the North Carolina Court of Appeals have held that the state constitution nonetheless includes a right to privacy that is similar to the constitutional right to informational privacy recognized in *Whalen*.[34]

Federal Laws and Regulations

The federal Privacy Act limits, but does not completely prohibit, the disclosure of personal information from most record systems maintained by federal agencies without the written consent of the individual to whom the record pertains.[35] The act generally does not apply to state or local government agencies—even if those agencies receive federal funding.[36]

The federal Freedom of Information Act (FoIA) requires most federal agencies to make information in their records available to the public. But it also allows federal agencies to refuse to release information or records if (1) disclosure would constitute a clearly unwarranted invasion of privacy or (2) the records are considered confidential or protected from disclosure under a federal statute (other than the Privacy Act).[37] The FoIA applies only to federal agencies; it does not apply to state or local governments.

A number of federal laws impose privacy requirements on state and local governments as a condition of receiving federal funding. The federal Family Educational Rights and Privacy Act (FERPA), for example, prohibits the U.S. Department of Education from providing federal funding to educational institutions whose policies or practices regarding the release of personally identifiable information contained in student education records do not comply with FERPA's confidentiality requirements.[38]

Other federal laws impose confidentiality requirements that are not tied to federal funding. For example, the federal Computer Matching and Privacy Protection Act of 1988 restricts the use and redisclosure of personal information that state and local social services agencies receive from federal record systems for use in computerized data-matching programs.[39] Similarly, one provision of the federal Privacy Act limits, but does not completely negate, the authority of state and local governments to require individuals to disclose their Social Security numbers in connection with their exercise of any right, benefit, or privilege provided by law.[40] The federal Videotape Privacy Protection Act prohibits businesses that are engaged in the rental or sale of videotaped movies from disclosing information that personally identifies

Many Web sites use encryption software to protect the information that passes across the Internet.

the specific videotaped materials rented or bought by consumers unless the disclosure is allowed under the act.[41] And the federal regulations on medical privacy adopted pursuant to the Health Insurance Portability and Accountability Act (discussed further in the article that begins on page 44) apply to virtually all health care providers and health care plans.[42]

State Statutes

North Carolina's General Assembly has enacted a number of statutes restricting the collection, use, or disclosure of personal information by state and local governments. For example, the state's Financial Privacy Act limits, but does not completely preclude, access by state and local government agencies to customers' financial records maintained by banks and other financial institutions.[43] Further, state statutes limit the disclosure by state and local government agencies of information from agency records regarding individual taxpayers, children involved in juvenile court proceedings, people who apply for or receive public assistance or services from county social services agencies, and public employees.[44]

North Carolina law also protects privacy by limiting disclosure of certain types of personal information collected by businesses, professionals, or individuals. For example, state rules governing the licensing of attorneys, doctors, psychologists, and other professionals often impose restrictions regarding the disclosure of confidential information about clients or patients.[45] Further, state statutes provide that "privileged" communications between clients, patients, or other specified types of individuals, and doctors, psychologists, clergy, or other specified categories of people generally may not be admitted as evidence in legal proceedings.[46] Other state laws restrict the disclosure of patients' prescription records by pharmacists, the disclosure of patients' records by public or private mental health facilities, the disclosure by any person that another person has HIV or AIDS, and the disclosure of library users' records by public libraries and private libraries that are open to the public.[47] In at least one instance, state law recognizes and protects a right to privacy with respect to personal solitude and repose by limiting the time and the manner of telephone solicitation calls.[48]

On the other hand, some state statutes *limit* privacy by requiring the release of information to state or local government agencies even if the information might otherwise be considered confidential. For example, state law generally requires individuals, businesses, professionals, and government agencies to share information with county social services agencies in cases involving child abuse and neglect or child support enforcement.[49]

Common Law

Courts in other states have recognized four distinct common law rights to privacy that protect individuals against

- unreasonable public disclosure of their private information;
- unreasonable intrusion on their solitude or seclusion or into their private affairs;
- misappropriation of their likenesses or identities; and
- being placed in a false light before the public.

North Carolina's courts have recognized a common law right to privacy for claims based on the misappropriation of an individual's name or likeness and on intrusion on solitude or seclusion.[50] But they have refused to recognize common law privacy claims based on placing an individual in a false light or claims involving the public disclosure of private information.[51] On the other hand, North Carolina law recognizes legal claims based on the improper disclosure by attorneys, doctors, or other professionals of confidential information regarding their clients or patients, as well as claims based on a person's (or, perhaps, a government employee's or agency's) intentional or negligent infliction of emotional distress by unreasonably disclosing personal information about an individual.[52]

Summary

Privacy is clearly an important public issue and a primary value of an open society—a value that has been recognized, protected, and sometimes limited by law. Privacy also is a multifaceted concept, sometimes confusing and complicated and not always clearly understood.

This article has provided a brief overview of the meaning of privacy, the individual and social interests that privacy serves, the competing public interests that may limit individual privacy, and the nature and the sources of legal rights to privacy. Other articles in this issue examine in more detail how privacy laws may affect state and local government agencies and officials.

Notes

1. The case referred to in the first panel on page 6 is Kyllo v. United States, 121 S. Ct. 2038 (2001). For a further discussion of it, see the article on page 13.

2. Judith Wagner DeCew, In Pursuit of

PRIVACY: LAW, ETHICS, AND THE RISE OF TECHNOLOGY 1–2, 145–64 (Ithaca, N.Y.: Cornell Univ. Press, 1997); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 69 (Chapel Hill: The Univ. of N.C. Press, 1995).

3. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARVARD LAW REVIEW 193 (1890).

4. *See* Osborn v. United States, 385 U.S. 323 (1966).

5. *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY 187 (New York: Basic Books, 1999).

6. *See* DECEW, IN PURSUIT OF PRIVACY; DAVID M. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY (New York: Praeger, 1979); VINCENT J. SAMAR, THE RIGHT TO PRIVACY: GAYS, LESBIANS, AND THE CONSTITUTION (Philadelphia: Temple Univ. Press, 1991).

7. DECEW, IN PURSUIT OF PRIVACY, at 58; O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY, at 232; SAMAR, THE RIGHT TO PRIVACY, at 19.

8. THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (Chicago: Callaghan & Co., 1880).

9. Olmstead v. United States, 277 U.S. 438, 478 (1928).

10. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (New York: Atheneum, 1967). The right to control access to personal information encompasses the right to control *what information* is known to others and *who* knows it.

11. DECEW, IN PURSUIT OF PRIVACY, at 46–60; SAMAR, THE RIGHT TO PRIVACY, at 51–60.

12. DECEW, IN PURSUIT OF PRIVACY, at 1.

13. *Id.*, at 27; SAMAR, THE RIGHT TO PRIVACY, at 14–18.

14. Of course, people differ in their experiences, feelings, needs, expectations, and actions with respect to personal privacy. For example, some people refuse to buy anything over the Internet or use cell phones because they fear that their credit card numbers or other personal information will be intercepted or disclosed. Others "blithely give out their credit-card numbers," Social Security numbers, or other personal information to government agencies and businesses. CHARLES J. SYKES, THE END OF PRIVACY 11, 13–15 (New York: St. Martin's Press, 1999).

15. ETZIONI, THE LIMITS OF PRIVACY, at 210.

16. Richard Posner, *An Economic Theory of Privacy*, in PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 333, 337–38 (Ferdinand D. Schoeman ed., Cambridge, Eng.: Cambridge Univ. Press, 1983).

17. DECEW, IN PURSUIT OF PRIVACY, 64, 67.

18. The federal Privacy Act (discussed later in text) expressly recognizes that an individual's legal rights and opportunities with respect to employment, insurance, and credit may be endangered by the disclosure of personal information. *See also* Mark I. Soler & Clark M. Peters, *Who Should Know What? Confidentiality and Information Sharing in Service Integration*, RESOURCE BRIEF, No. 3 (New York: Nat'l Center for Service Integration, 1993); MARK I. SOLER *et al.*, GLASS WALLS: CONFIDENTIALITY PROVISIONS AND INTERAGENCY COLLABORATIONS (San Francisco: Youth Law Center, 1993).

19. DECEW, IN PURSUIT OF PRIVACY, at 69–70; JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 215–16 (New York: Random House, 2000); John L. Saxon, *Confidentiality and Social Services (Part I): What Is Confidentiality?* SOCIAL SERVICES BULLETIN, No. 30, at 32–39 (Chapel Hill: Inst. of Gov't, The Univ. of N.C. at Chapel Hill, 2001).

20. REGAN, LEGISLATING PRIVACY, at 23, 221, 223.

21. LEGAL ACTION CENTER, CONFIDENTIALITY AND COMMUNICATION 4 (New York: Legal Action Center, 2000).

22. WESTIN, PRIVACY AND FREEDOM, at 32–39; Whalen v. Roe, 429 U.S. 589, 605–06 (1977).

23. O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY, at 19.

24. ETZIONI, THE LIMITS OF PRIVACY, at 4.

25. *Id.*; O'BRIEN, PRIVACY, LAW, AND PUBLIC POLICY, at 20, 27; Saxon, *What Is Confidentiality?* at 7–9.

26. FERPA, for example, allows the disclosure of information from student records for "directory" purposes (say, in a university's student directory); to school personnel for legitimate educational purposes; when disclosure is necessary to protect health or safety; pursuant to court order; or for other purposes specified in the statute. 20 U.S.C. § 1232g(b).

27. SYKES, THE END OF PRIVACY, at 246.

28. ETZIONI, THE LIMITS OF PRIVACY, at 4.

29. The legal bases of privacy and confidentiality are discussed in more detail in John L. Saxon, *Confidentiality and Social Services (Part II): Where Do Confidentiality Rules Come From?* SOCIAL SERVICES BULLETIN, No. 31 (Chapel Hill: Inst. of Gov't, The Univ. of N.C. at Chapel Hill, 2001).

30. In analyzing legal rights to privacy, it is important to identify the *subject* of the right (the people who hold the right), the *object* of the right (the types of information, decisions, or behaviors that are protected), the *respondents* (individuals, businesses, government agencies, or others) against whom the right may be asserted, and the *reason* (interest, policy, or justification) on which the right is based. *See* SAMAR, THE RIGHT TO PRIVACY, at 14–18.

31. *See* Katz v. United States, 389 U.S. 347 (1967). The North Carolina Constitution (Art. I, Sec. 20) also prohibits unreasonable searches by government agencies or officials.

32. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965); Roe v. Wade, 410 U.S. 113 (1973).

33. Whalen v. Roe, 429 U.S. 589, 605 (1977).

34. Treants Enter. v. Onslow County, 83 N.C. App. 345, 350 S.E.2d 365 (1986), *aff'd on other grounds*, 320 N.C. 776, 360 S.E.2d 783 (1987); ACT-UP Triangle v. Commission for Health Serv., 345 N.C. 699, 483 S.E.2d 388 (1997).

35. 5 U.S.C. § 552a.

36. St. Michael's Convalescent Hosp. v. California, 643 F.2d 1369 (9th Cir. 1981).

37. 5 U.S.C. § 552(b)(6). *See* United States Dep't of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989) (holding that disclosure of individual's FBI "rap sheet" would constitute unwarranted invasion of privacy under FoIA even though it contained information obtained from public records).

38. 20 U.S.C. § 1232g; 34 C.F.R. § 99.

39. 5 U.S.C. §§ 552a(a)(8)–(12), 552a(o)–(r).

40. 5 U.S.C. § 552a (note). *See* David M. Lawrence, *Local Government Requirements for and Use of Social Security Account Numbers*, LOCAL GOVERNMENT LAW BULLETIN, No. 55 (Chapel Hill: Inst. of Gov't, The Univ. of N.C. at Chapel Hill, 1994). *See also* G.S. 143-64.60.

41. 18 U.S.C. § 2710. Enacted under Congress's authority to regulate interstate commerce, this federal act preempts state laws that otherwise would allow or require the disclosure of protected information.

42. 65 Fed. Reg. 82,462 (Dec. 28, 2000); 45 C.F.R. pts. 160, 164.

43. G.S. 53B-1 through -10.

44. G.S. 105-259; G.S. 7B-302(b), -2901, -3000; G.S. 108A-80; G.S. 115C-319 through -321; G.S. 126-22 through -30, 153A-98, 160A-168.

45. *See, e.g.*, 27 N.C. ADMIN. CODE 2.1, r. 1.6; 21 N.C. ADMIN. CODE 63.0507.

46. *See, e.g.*, G.S. 8-53, -53.2, -53.3; Michael v. Foil, 100 N.C. 178, 6 S.E. 264 (1888).

47. G.S. 90-85.36; G.S. 122C-52 through -56; G.S. 130A-143; G.S. 125-19.

48. G.S. 75-30.1.

49. G.S. 7B-302(e); G.S. 110-139(d).

50. Miller v. Brooks, 123 N.C. App. 20, 25–26, 472 S.E.2d 350, 354 (1996); Flake v. Greensboro News Co., 212 N.C. 780, 790–93, 195 S.E. 55, 62–64 (1938).

51. Renwick v. News and Observer, 310 N.C. 312, 322, 312 S.E.2d 405, 411 (1984); Hall v. Post, 323 N.C. 259, 263–70, 372 S.E.2d 711, 714–17 (1989).

52. *See* Jones v. Asheville Radiological Group, 134 N.C. App. 528, 518 S.E.2d 528 (1999), *rev'd on other grounds*, 351 N.C. 348, 524 S.E.2d 804 (2000); *Hall*, 323 N.C. at 268, 372 S.E.2d at 716; Woodruff v. Miller, 64 N.C. App. 364, 307 S.E.2d 176 (1983); Burgess v. Busby, 142 N.C. App. 393, 399, 544 S.E.2d 4, 7 (2001).

The Fourth Amendment, Privacy, and Law Enforcement

Robert L. Farb

North Carolina appellate courts have upheld the constitutionality of checkpoints for driver's licenses.

GARY ALLEN / NEWS & OBSERVER

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation and particularly describing the place to be searched and the persons or things to be seized.

—U.S. Constitution, Amendment IV

Privacy . . . the right to be free from governmental interference . . . a law enforcement officer's authority to investigate crimes . . . the government's interest in investigating conduct that is not necessarily criminal—the Fourth Amendment affects all these issues.[1]

The Fourth Amendment protects people against unreasonable searches and seizures by government authorities. The U.S. Supreme Court, which must determine how the Fourth Amendment applies in a wide range of contexts, has sought to strike a balance between society's interest in investigating crime and individuals' interests in maintaining their privacy against government intrusion. The Fourth Amendment does not apply to activities by a private person, no matter how unjustified, unless the private person acts as an agent of government officials or acts with their participation or knowledge.

One U.S. Supreme Court case, *Katz v. United States*, has had a particularly important impact on the relationship between privacy and government authority under the Fourth Amendment, establishing the basic test for determining whether a person's interest in privacy is sufficient to warrant Fourth Amendment protection.[2] This and later cases decided by the Court—as well as federal and state legislation that expands on the basic protections afforded by the Fourth Amendment—are the focus of this article.[3]

Reasonable Expectation of Privacy under the Fourth Amendment

Charles Katz's occupation was illegal gambling. In February 1965 he was using several telephones in a bank of public telephone booths on Sunset Boulevard in Los Angeles to conduct his gambling business. The Federal Bureau of Investigation (FBI) learned of his activities and placed microphones and a tape recorder on the tops of the telephone booths and recorded his conversations—without obtaining a search warrant. He was convicted of gambling violations.

The appeal of his conviction eventually reached the U.S. Supreme Court. The government argued that no search occurred because the FBI had not physically penetrated the telephone booth to listen to Katz's conversations.[4] The Court's opinion, written by Justice Potter Stewart, rejected the government's argument. It said that the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his or her own home or office, is not protected by the Fourth Amendment. But what a person seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. The Court concluded that the government's activities in

The author is an Institute of Government faculty member who specializes in criminal law and procedure. Contact him at farb@iogmail.iog.unc.edu.

electronically listening to and recording Katz's conversations violated the privacy on which he justifiably relied while using the telephone booth, and thus violated the Fourth Amendment.

At least as significant as Justice Stewart's opinion was Justice John Harlan's concurring opinion, which used the term "reasonable expectation of privacy" and explained its meaning. Justice Harlan noted that the Court had ruled that an enclosed telephone booth is an area, like a home, where a person has a constitutionally protected reasonable expectation of privacy. He said that there is a two-fold requirement when determining if there is Fourth Amendment protection: (1) a person must have demonstrated an actual (subjective) expectation of privacy; and (2) the expectation must be one that society is prepared to recognize as reasonable. A person who enters a telephone booth, shuts the door, and places a call, Justice Harlan continued, is entitled to assume that his or her conversation is not being intercepted—per the first test just stated. And although an enclosed telephone booth is accessible to the public at times, its occupant's expectation of freedom from intrusion when inside the booth is one that society recognizes as reasonable—per the second test. Later Supreme Court cases have adopted the reasonable-expectation-of-privacy analysis for determining whether people's activities are protected from governmental intrusion under the Fourth Amendment.[5]

Government Actions Subject to the Fourth Amendment

The *Katz* test provides a starting point for determining the extent of the Fourth Amendment's protections: the amendment applies when a person has a reasonable expectation of privacy. Other court decisions have developed rules detailing how the Fourth Amendment regulates government conduct in specific situations. Those rules are the subject of this section.

Street Encounters

Little did Detective Martin McFadden know when he was patrolling downtown Cleveland, Ohio, on the afternoon of October 31, 1963, that his encounter with John Terry would lead to the U.S. Supreme Court's most significant ruling expanding a law enforcement officer's authority to investigate criminal activity.

Detective McFadden, a police officer for thirty-nine years and a detective for thirty-five years, had been patrolling downtown Cleveland for shoplifters and pickpockets for thirty years. His attention was drawn to two men, Richard Chilton and John Terry, standing at an intersection. He later testified that "they didn't look right to me at the time."[6] McFadden decided to observe them from a distance of 300 to 400 feet. The two men took turns walking past store windows and looking into a particular one. Then they conferred briefly. They repeated this ritual five or six times apiece—in all, making about a dozen trips. A third man approached them, engaged them briefly in conversation, then walked away. Chilton and Terry resumed their measured pacing, peering, and conferring. After about ten minutes, they walked off together in the same direction as the third man.

McFadden now had become suspicious that they were casing a store to commit a robbery. He feared that they might have a gun. He followed the two men and saw them stop in front of the store to talk to the same man with whom they had conferred earlier. McFadden approached them, identified himself as a police officer (he was in plain clothes), and asked for their names. When the men mumbled something in response to his inquiries, McFadden grabbed Terry—spun him around so that he and McFadden were facing the other two—and patted down the outside of his clothing. He felt a pistol in the left breast pocket of Terry's overcoat, which he removed after securing all three men. Terry was convicted of carrying a concealed weapon. The appeal of his conviction eventually reached the U.S. Supreme Court.

Chief Justice Earl Warren wrote the Court's opinion in *Terry v. Ohio*, which decided several significant issues:[7]

- Stopping and frisking are subject to the Fourth Amendment even though those actions may not be as intrusive as an arrest or a full search of a person. The Court found that in forcibly stopping Terry by grabbing him, Detective McFadden seized him, and that in patting down the outer surfaces of Terry's clothing, McFadden searched him. The Court recognized that both the seizure (the forcible stop) and the search (the frisk) were actions regulated by the Fourth Amendment.
- The Court noted that if this case involved law enforcement conduct subject to the Warrant Clause ("no Warrants shall issue but upon probable cause . . .") of the Fourth Amendment, then the Court would have to determine whether probable cause existed to justify McFadden's search and seizure of Terry. To determine whether probable cause was the appropriate standard, the court used a balancing test: evaluating the officer's need to search or seize against the invasion of privacy that the search or seizure entailed.[8] The Court decided that officer safety outweighed the intrusion on a person's freedom when frisked for weapons, and a standard less than probable cause was reasonable under the Fourth Amendment's general proscription of unreasonable searches and seizures. This standard became known in later cases as "reasonable suspicion."[9]
- The Court determined that, in light of McFadden's experience as a law enforcement officer, the information he possessed supported his frisk of Terry for weapons. Also, the Court ruled, the scope of the frisk—patting Terry's outer clothing—was properly confined to what was necessary to learn whether he was armed. That is, McFadden did not conduct an impermissible general exploratory search for evidence of criminal activity.

As he had done in *Katz v. United States*, Justice Harlan wrote a significant concurring opinion. The Court's opinion did not specifically address whether the forcible stop of McFadden was lawful. Justice Harlan made clear his view, however, that an officer may forcibly stop a person before frisking him or her for weapons, and the standard for that stop also is less than probable cause.

When officers have lawfully stopped a vehicle, they may order both the driver and passengers out of it. To frisk an occupant, they need at least reasonable suspicion that the person is armed and presents a danger.

The Court in later cases recognized that an officer may make a forcible stop of a person or a vehicle on the basis of reasonable suspicion of criminal activity.[10]

The Home and Its Curtilage

The U.S. Supreme Court has stated that the "physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed" and that "searches and seizures inside a home without a warrant are presumptively unreasonable."[11] Thus a law enforcement officer may not enter a home without a warrant unless (1) the officer has consent to enter or (2) exigent circumstances (a need for immediate action) justify entering without consent or a warrant.

Entering a residence to arrest. Without consent or exigent circumstances, an officer needs an arrest warrant to enter the residence of a person to be arrested. Without consent or exigent circumstances, an officer who wants to enter the home of a third party to arrest a person who does not live there must have a search warrant. An arrest warrant is insufficient to enter a third party's home because it does not adequately protect the third party's Fourth Amendment privacy interests.[12]

Entering the curtilage. People have a reasonable expectation of privacy not only in their home but also in its curtilage.[13] The "curtilage" is the area immediately surrounding the home, so intimately tied to the home itself that it deserves Fourth Amendment protection —for example, the area that includes buildings like an unattached garage, a storage shed, and similar structures, if they are relatively close to the dwelling and serve the homeowner's daily needs.

Officers who enter the curtilage without a warrant, consent, or exigent circumstances conduct an impermissible search under the Fourth Amendment except when they go to a house by using the common entranceway (for example, a driveway or a sidewalk leading to a door) for a legitimate purpose, such as to question a suspect in a criminal investigation. A person ordinarily expects a variety of people to enter private property for any number of reasons. Therefore a person does not have a reasonable expectation of privacy in the areas of private property commonly used by those who come there.[14]

Entering areas outside the curtilage. When officers are on private property *outside* the curtilage—for example, when they are walking through fields or woods—they are not conducting a search under the Fourth Amendment because the U.S. Supreme Court has ruled that a person has no reasonable expectation of privacy in the area outside the curtilage.[15] The Fourth Amendment does not protect that area even if officers are committing a criminal trespass or even if the area is surrounded by a fence with no-trespassing signs.[16] However, a person may have a reasonable expectation of privacy in an enclosed building located there.[17]

Using devices to detect activity within a home. Officers suspected that marijuana was being grown in Danny Kyllo's home. Growing marijuana indoors typically requires high-intensity lamps. Officers parked their car on the street near his home and—without obtaining a search warrant—used a thermal imager to determine whether the amount of heat emanating from the home was consistent with the use of such lamps. The imager showed that the roof over the garage and a side wall of the home were relatively hot compared with the rest of the home and substantially warmer than neighboring homes. On the basis of this and other information, the officers obtained a search warrant. In *Kyllo v. United States*, the U.S. Supreme Court ruled that using sense-enhancing technology to obtain any information concerning the interior of a home (in this case, the relative heat of various rooms) that could not have been obtained without physical intrusion into a constitutionally protected area is a search under the Fourth Amendment —at least when the technology is not in general public use.[18] Thus the officers in

this case violated Kyllo's Fourth Amendment rights by using a thermal imager without first having obtained a search warrant.[19]

The *Kyllo* ruling makes clear that the Court will likely consider to be a search the use of other technological instruments as intrusive as a thermal imager to reveal private matters within a home. It remains unclear whether the Court will rule differently if and when certain technological instruments become widely used by the general public.[20]

Flying over a home and its curtilage. Generally, aircraft surveillance is permissible to help officers make observations and does not constitute a search under the Fourth Amendment. For example, officers do not conduct a search when they fly in lawful navigable airspace over a home and its curtilage and see with their unaided eyes marijuana plants in a fenced-in yard. The U.S. Supreme Court has ruled that a person does not have a reasonable expectation of privacy from observations from an aircraft in public airspace at an altitude at which the public travels with sufficient regularity—because any person flying in such airspace who looks down can see what officers can see.[21] However, officers' actions may constitute a search, requiring appropriate justification—usually a search warrant—if they also use sophisticated cameras and the like to see intimate activities within a home or its curtilage that they could not see unaided.

Officers may fly aircraft at any altitude over open fields because, as with areas outside the curtilage of his or her home, a person does not have a reasonable expectation of privacy there.

Sorting through garbage. The U.S. Supreme Court has ruled that people do not have a reasonable expectation of privacy in garbage that they have placed for collection on the curb in front of their house.[22] The Court reasoned that garbage left on or at the side of a public street is readily accessible to scavengers and other members of the public. Moreover, people are aware when placing their trash for pickup by a third party—for example, sanitation workers—that these workers may sort through the garbage or permit others, including law enforcement officers, to do so.[23] Garbage placed for collection in an area accessible to the public is not subject to an expectation of privacy that society recognizes as reasonable.

Motor Vehicles

Stopping motor vehicles on a highway or at a checkpoint. The U.S. Supreme Court has ruled that an officer may not stop a car traveling on a highway simply to check the operator's driver's license. To stop a vehicle, an officer generally needs reasonable suspicion that the driver has violated a law.[24] Using the Fourth Amendment's balancing test from *Terry v. Ohio*, discussed earlier, the Court concluded that the marginal contribution to highway safety resulting from this kind of license check cannot justify subjecting all vehicle drivers to being stopped at the unbridled discretion of law enforcement officers.

However, in the same opinion, the Court indicated that driver's license checkpoints would be constitutional.[25] A typical checkpoint is set up at a designated place on a highway, and all cars are stopped to check driver's licenses.[26] Reasonable suspicion of a driver's license violation, another traffic violation, or criminal activity is not required to stop a car at the checkpoint. Most state appellate courts, including North Carolina's, have upheld such checkpoints.[27]

The U.S. Supreme Court also has upheld the validity of checkpoints for impaired drivers.[28] Using the Fourth Amendment's balancing test, the Court concluded that the state's interest in combating impaired driving outweighs the intrusion on motorists of being briefly stopped at these checkpoints.

On the other hand, the Court has ruled unconstitutional a vehicle checkpoint whose primary purpose is to detect illegal drugs.[29] The Court noted that it had approved checkpoints to deal with highway safety or to police the nation's border.[30] But if it approved a checkpoint to detect illegal drugs, law enforcement officers could establish checkpoints for any conceivable law enforcement purpose.[31] The Court's application of the balancing test under the Fourth Amendment was resolved in favor of an individual's right to be free from governmental intrusion.

Ordering the driver and passengers out of a vehicle. According to the U.S. Supreme Court, when officers have lawfully stopped a vehicle, they may order the driver and passengers out of it without articulating any reason for doing so.[32] Using the Fourth Amendment's balancing test, the Court concluded that the strong governmental interest in an officer's protection from assault by weapons that may be in a car outweighs the minimum intrusion on drivers and passengers when required to exit a car.

Searching a vehicle with probable cause but no search warrant. When officers have probable cause to search a vehicle for evidence of a crime, and the vehicle is in a public place (that is, a place where a person does not have a reasonable expectation of privacy), they may seize the vehicle—whether it is moving or parked—without a search warrant. Also, they may search it where they seized it or take it to a law enforcement facility or another place and search it there.[33]

This legal principle is an exception to the general rule that officers may make a warrantless search with probable cause only when exigent circumstances justify a failure to obtain a search warrant—for example, when the evidence might disappear if they took the time to obtain a warrant. The U.S. Supreme Court and the North Carolina Supreme Court have justified this principle on the ground that people have a lesser expectation of privacy in their vehicles than in their homes because government pervasively regulates vehicles.[34]

Government Conduct Subject to Other Laws

Federal and state laws may go farther than the floor established by the Fourth Amendment, applying, for example, to private activities. The following sections highlight two areas covered by federal and state laws.

Wiretapping and Eavesdropping

Wiretapping and eavesdropping are pervasively regulated by federal and state laws. Therefore most of this discussion is based on these laws.[35] Although the Fourth Amendment is clearly implicated in many aspects of wire-

Garbage placed at the curb for collection is fair game for law enforcement officers to search.

tapping and eavesdropping, there have been relatively few Fourth Amendment rulings because federal and state laws are as restrictive as, and sometimes more restrictive than, the Fourth Amendment. These laws are quite complex, and this discussion will attempt to cover only some of the basic issues.[36]

An important point to be made at the outset about these laws is that they often apply to private people's activities as well as governmental activities, whereas the Fourth Amendment applies only to the latter. Thus anyone who violates these laws may be subject to criminal and civil penalties.

Intercepting telephone conversations. Generally, it is unlawful to use a device to intercept a telephone conversation (as well as voice communications over pagers).[37] The law applies not only to regular telephones but also to cellular and cordless telephones—even though conversations on some of the latter may be intercepted by scanners and radios that many people own and use.

North Carolina law enforcement officers may intercept telephone conversations, but they must obtain a special court order from a designated court, and the requirements for obtaining the court order are significantly more stringent than those for obtaining a search warrant.[38]

However, neither federal nor North Carolina law makes it unlawful to tape-record a telephone conversation in which one party to the conversation has given prior consent to its being tape-recorded.[39] For example, law enforcement officers may tape-record (1) a telephone conversation between themselves and a criminal suspect or (2) a telephone conversation between a government informant with a criminal suspect when the informant has given prior consent. (However, a person's Sixth Amendment right to counsel may bar this activity under certain circumstances.)[40] Also, a private person may tape-record a telephone conversation between himself or herself and another party to the conversation.[41] However, a spouse may not install a device on a telephone to tape-record his or her spouse's telephone conversations with third parties unless the other spouse has given prior consent.[42]

Using a device to intercept oral communication. It is illegal under federal and state law to use a device to intercept an oral communication under circumstances in which a person has a reasonable expectation of privacy. This is the same standard as the Fourth Amendment standard adopted in *Katz v. United States*.[43] Thus a person who places an eavesdropping device in a bedroom to listen to or to record oral communications violates federal and state law—assuming, of course, that a party to the communications did not give prior consent to the use of the device there. On the other hand, a person who secretly records an open city council meeting does not violate federal or state law because council members and other speakers do not have a reasonable expectation of privacy that their statements will not be recorded by others.

As with telephone conversations, a law enforcement officer or a private person does not violate federal or state law when he or she surreptitiously tape-records a conversation with another person if one party to the conversation has given prior consent to the recording.[44] The U.S. Supreme Court and the North Carolina Supreme Court also have ruled that a law enforcement officer's conduct under these circumstances does not violate the Fourth Amendment because a person does not have a reasonable expectation of privacy in a conversation with another person who happens to be a law enforcement officer or an agent of the officer.[45] A person contemplating criminal activity takes the risk that the person with whom he or she is conversing is an officer or someone who may report the conversation to an officer.

Intercepting or reading electronic mail (e-mail). Officers may not intercept and read an e-mail message during its

transmission without a special court order, as described earlier for interception of telephone conversations.[46] However, an officer does not need a special court order once the message has been transmitted. If a message has been unopened for 180 days or less, only a search warrant is necessary to read it.[47] If a message has been opened, or if it remains unopened for more than 180 days, then an officer may read the message by obtaining a search warrant or, with notice to the recipient of the message, by obtaining a subpoena or a court order.[48] The law allows delayed notice to the recipient under certain circumstances.[49]

Neither federal nor North Carolina law makes it unlawful to tape-record a telephone conversation in which one party to the conversation has given prior consent to its being tape-recorded.

Additional provisions allow a law enforcement officer to obtain subscriber information.[50] Further, they sometimes permit service providers to disclose information to officers voluntarily.[51]

Conducting video surveillance. Nonaural video surveillance (surveillance that does not record oral communications) is not regulated by federal or state wiretapping or eavesdropping laws.[52] However, video surveillance directed at places where a person has a reasonable expectation of privacy is a search under the Fourth Amendment, and usually a search warrant is required to conduct the surveillance.[53] For example, officers need a search warrant to place a nonaural video camera on a utility pole to record all activities in a person's backyard, when the backyard is surrounded by a ten-foot-high fence.[54] On the other hand, a nonaural video camera directed at people on a public street or sidewalk to observe possible drug transactions does not implicate anyone's reasonable expectation of privacy and may be used without a search warrant or other legal authorization.

Records in a Third Party's Possession

The U.S. Supreme Court has ruled that a person does not have a reasonable expectation of privacy in his or her bank records.[55] The Court reasoned that, in revealing his or her financial affairs to another, a bank customer takes the risk that the information will be conveyed by that person or institution to the government. However, the North Carolina General Assembly has enacted legislation that requires law enforcement officers to obtain appropriate legal process (a search warrant, a court order, or a subpoena) to obtain bank records.[56]

A U.S. Supreme Court case makes clear that a person does not have a reasonable expectation of privacy in his or her telephone records, including telephone numbers dialed from or to a telephone.[57] However, Congress has enacted legislation that requires law enforcement officers to obtain appropriate legal process to obtain telephone records.[58] Further, the North Carolina General Assembly has enacted legislation requiring a law enforcement officer to obtain a court order to use a device that records numbers dialed from or to a telephone.[59]

Many other records, such as personnel or school records, are subject to federal and state laws regulating disclosure. The protections for those records are discussed elsewhere in this issue of *Popular Government* (see pages 33 and 36).

Conclusion

This article has briefly surveyed some privacy and law enforcement issues involved with the Fourth Amendment and federal and state legislation. With constant technological advances, debate will become more intense about the proper balance between a person's right to privacy and the government's need to investigate crimes. These issues will be the subject of future court decisions and federal and state legislative activity that will continue to define the scope of individual privacy and law enforcement authority.

Notes

1. Examples of the government's interest in investigating conduct that is not necessarily criminal are workplace and school searches, discussed elsewhere in this issue of *Popular Government*; see pages 33 and 36.

2. Katz v. United States, 389 U.S. 347 (1967).

3. For a more detailed discussion of Fourth Amendment issues, *see* ROBERT L. FARB, ARREST, SEARCH, AND INVESTIGATION IN NORTH CAROLINA (2d ed., Chapel Hill: Inst. of Gov't, The Univ. of N.C. at Chapel Hill, 1993) and ROBERT L. FARB, 1997 SUPPLEMENT TO ARREST, SEARCH, AND INVESTIGATION IN NORTH CAROLINA (Chapel Hill: Inst. of Gov't, The Univ. of N.C. at Chapel Hill, 1998). A new edition of ARREST, SEARCH, AND INVESTIGATION is expected in 2003.

4. The government's argument relied on Olmstead v. United States, 277 U.S. 438 (1928), and Goldman v. United States, 316 U.S. 129 (1942).

5. *See, e.g.*, Oliver v. United States, 466 U.S. 170 (1984).

6. Terry v. Ohio, 392 U.S. 1, 5 (1968).

7. *Terry*, 392 U.S. 1.

8. The Court adopted the balancing test from Camara v. Municipal Court, 387 U.S. 523 (1967), which ruled that conducting a routine building inspection without a warrant or consent violated the Fourth Amendment. As a result of that ruling, the North Carolina General Assembly enacted Section 15-27.2 of the NORTH CAROLINA GENERAL STATUTES (hereinafter G.S.), which requires an administrative inspection warrant to conduct such an inspection.

9. United States v. Brignoni-Ponce, 422 U.S. 873 (1975).

10. Adams v. Williams, 407 U.S. 143 (1972); United States v. Cortez, 449 U.S. 411 (1981).

11. Payton v. New York, 445 U.S. 573, 585–86 (1980).

12. *See* FARB, ARREST, SEARCH, AND INVESTIGATION, at 48–52, and FARB, SUPPLEMENT, at 9.

13. *See* FARB, ARREST, SEARCH, AND INVESTIGATION, at 86–87.

14. *See id.* at 87. Officers who are conducting a legitimate law enforcement function on private property are not violating North Carolina's criminal trespass laws. *See* FARB, ARREST, SEARCH, AND INVESTIGATION, at 117 n.99.

15. Oliver v. United States, 466 U.S. 170 (1984).

16. *See* FARB, ARREST, SEARCH, AND INVESTIGATION, at 87, 117 n.99.

17. State v. Tarantino, 322 N.C. 386, 368 S.E.2d 588 (1988).

18. Kyllo v. United States, 533 U.S. 27 (2001).

19. If exigent circumstances exist, then a search warrant is not required. For example, if a person is holding hostages within a home in a life-threatening situation, officers may use sense-enhancing equipment if they believe it will be useful in locating people in the home.

20. Even if the Court ruled that the Fourth Amendment would not bar use of certain technological instruments, Congress or state legislatures could legislate otherwise. For example, in 1994, Congress made it unlawful to intercept, without a court order, the radio portion of a cordless telephone communication transmitted between the cordless telephone handset and its base unit. Act of Oct. 25, 1994, Pub. L. No. 103-414, § 202(a), 108 Stat. 4290 (1994). At the time some courts had held that a person did not have a reasonable expectation of privacy in such conversations, which were readily overheard by people with scanners or radio receivers. *See, e.g.,* Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989); Price v. Turner, 260 F.3d 1144 (9th Cir. 2001).

21. California v. Ciraolo, 476 U.S. 207 (1986); Florida v. Riley, 488 U.S. 445 (1989). Flying over business premises is analyzed differently. *See* Dow Chemical Co. v. United States, 476 U.S. 227 (1986).

22. California v. Greenwood, 486 U.S. 35 (1988).

23. Officers also may make arrangements with sanitation workers to collect trash at a person's residence and give it to the officers. State v. Hauser, 342 N.C. 382, 464 S.E.2d 443 (1995).

24. Delaware v. Prouse, 440 U.S. 648 (1979).

25. *Id.* at 663. More recently the Court noted the likely constitutionality of such checkpoints in City of Indianapolis v. Edmond, 531 U.S. 32 (2000).

26. Typically all cars are stopped except when traffic congestion requires that some cars be waived through.

27. State v. Sanders, 112 N.C. App. 477, 435 S.E.2d 842 (1993); State v. Tarlton, 146 N.C. App. 417, 553 S.E.2d 50 (2001).

28. Michigan Dept. of State Police v. Sitz, 496 U.S. 444 (1990). G.S. 20-16.3A authorizes checkpoints for impaired drivers.

29. *Edmond*, 531 U.S. at 32. The Court in *Edmond* specifically did not decide whether a checkpoint would be unconstitutional if the primary purpose was permissible—for example, to check for impaired drivers—and a secondary purpose was to check for illegal drugs.

30. *Sitz*, 496 U.S. 444 (checkpoints to deal with highway safety); United States v. Martinez-Fuerte, 428 U.S. 543 (1976) (checkpoints to police the nation's border).

31. The Court recognized, however, the constitutionality of roadblocks set up immediately after the commission of a crime, such as a bank robbery, to stop a fleeing suspect.

32. Pennsylvania v. Mimms, 434 U.S. 106 (1977) (driver); Maryland v. Wilson, 518 U.S. 408 (1997) (passengers).

33. State v. Isleib, 319 N.C. 634, 356 S.E.2d 573 (1987) (decided under both U.S. and North Carolina constitution); California v. Carney, 471 U.S. 386 (1985); United States v. Johns, 469 U.S. 478 (1985); Michigan v. Thomas, 458 U.S. 259 (1982); Texas v. White, 423 U.S. 67 (1975); Chambers v. Moroney, 399 U.S. 42 (1975).

34. California v. Carney, 471 U.S. 386 (1985); State v. Isleib, 319 N.C. 634, 356 S.E.2d 573 (1987). Although the Court also has stated that a vehicle's mobility is another reason to permit a warrantless search, that reason hardly has much force when the Court permits a warrantless search even after a vehicle and its contents have been immobilized.

35. *See generally* 18 U.S.C.A. §§ 2510–2522, 2701–2711, and G.S. 15A-286 through -298.

36. A useful publication is CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING (2d ed., Deerfield, Ill.: Clark Boardman Callaghan, 1995). The most current supplement, published by West Group, was issued in August 2001.

37. "Intercept" is defined in both federal and state law as "the aural or other acquisition of the contents of any wire, oral, or electronic communication through the use of any electronic, mechanical, or other device." 18 U.S.C.A. § 2510(4); G.S. 15A-286(13).

38. *See* FARB, SUPPLEMENT, at 16–17.

39. 18 U.S.C.A. § 2511(c), (d); G.S. 15A-287(a). However, such tape-recording is illegal under federal law if a private person intercepts a communication to commit a crime or a tortuous act (a civil wrong). Some states allow the tape-recording of a conversation only under limited circumstances, or prohibit it unless all the parties to the conversation have consented. *See* FISHMAN & MCKENNA, WIRETAPPING AND EAVESDROPPING §§ 6:15 through 6:28; 6:38.

40. *See* FARB, ARREST, SEARCH, AND INVESTIGATION, at 218–23. Generally, officers may not deliberately elicit statements from a defendant—whether in custody or not—after his or her Sixth Amendment right to counsel for a criminal charge becomes operative. This right begins for a felony charge after a defendant's first appearance in district court or a defendant's indictment, whichever occurs first. Thus, for example, law enforcement officers who by themselves or through an informant deliberately elicit statements in a telephone conversation (whether recorded or not) from a defendant after his or her indictment may violate the defendant's Sixth Amendment right to counsel.

41. See note 39.

42. State v. Rickenbacher, 290 N.C. 373, 226 S.E.2d 347 (1976); State v. Shaw, 103 N.C. App. 268, 404 S.E.2d 887 (1991).

43. 18 U.S.C.A. § 2510(2); G.S. 15A-286(17) (definition of "oral communication"). *See* United States v. Turner, 209 F.3d 1198 (10th Cir. 2000); *In re* John Doe Trader Number One, 894 F.2d 240 (7th Cir. 1990); Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989); United States v. Harrelson, 754 F.2d 1153 (5th Cir. 1985).

44. See note 39.

45. United States v. White, 401 U.S. 745 (1971); State v. Levan, 326 N.C. 155, 388 S.E.2d 429 (1990). There is no Fourth Amendment issue when a private person records the conversation because the amendment applies only to the government and its agents.

46. The discussion in this section concerns obtaining information from a public service provider, such as America Online or Microsoft. The laws are somewhat different for nonpublic service providers.

47. 18 U.S.C.A. § 2703(a).

48. 18 U.S.C.A. § 2703(b).

49. 18 U.S.C.A. § 2705.

50. 18 U.S.C.A. § 2703(c).

51. For example, a service provider may divulge the contents of a communication to a law enforcement agency if the provider inadvertently obtained the communication and it appeared to pertain to the commission of a crime. 18 U.S.C.A. § 2702(b)(6).

52. United States v. Falls, 34 F.3d 674 (3d Cir. 1997).

53. It would be extremely unusual if a person who was present during the entire video surveillance had given prior consent to it or if exigent circumstances existed to excuse the requirement of a search warrant.

54. United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987). Some courts have imposed rigorous requirements for search warrants for video surveillance. *See, e.g.,* United States v. Koyomejian, 970 F.2d 536 (9th Cir. 1992).

55. United States v. Miller, 425 U.S. 435 (1976).

56. G.S. 53B-1 through -10. *See also* FARB, ARREST, SEARCH, AND INVESTIGATION, at 85.

57. Smith v. Maryland, 442 U.S. 735 (1979). Although the *Smith* Court ruled only that a person does not have a reasonable expectation of privacy in telephone numbers that a person dials on his or her telephone, the ruling clearly would also apply to telephone numbers dialed to that telephone and to telephone records maintained by the telephone company.

58. *See* FARB, ARREST, SEARCH, AND INVESTIGATION, at 86.

59. G.S. 15A-260 through -264. *See also* FARB, ARREST, SEARCH, AND INVESTIGATION, at 84–85. A "pen register" records numbers dialed from a telephone, and a "trap-and-trace device" records numbers dialed to a telephone.

An Overview of Protected and Public Information in North Carolina

David M. Lawrence

North Carolina law reflects a strong general policy of openness in governmental operations, expressed in its public records and open meetings statutes. Because of these statutes, the great mass of public records, especially the business records of government, is open to public access, and most meetings of most public bodies in North Carolina are conducted entirely in public.[1]

Almost all citizens applaud these statutory policies, which North Carolina shares with the other forty-nine states. Sometimes, however, the statutes permit public access to governmental meetings, and especially to governmental records, with results that at least some people consider invasive of their privacy. A client of a community development agency or a person whose occupation is regulated by a state licensing board might suddenly begin receiving junk mail because an advertiser has acquired the agency's list of clients or the licensing board's list of licensees through a public records request. Or a citizen who has written a letter to her city's manager might find it published in the local newspaper, which has obtained a copy pursuant to the public records law.

Nothing in the public records statute protects the people in the preceding examples whose sense of privacy has been violated. The General Assembly has, however, created numerous exceptions to the general demands of openness established in the public records and open meetings statutes. And in most cases it has done so because of concerns about privacy: almost all the exceptions to both statutes can be explained, at least in part, as legislative recognition of the legitimacy of certain claims of privacy. What kinds of information, then, do these exceptions protect?

The author is an Institute of Government faculty member whose specialties include public records and open meetings laws. Contact him at lawrence@iogmail.iog.unc.edu.

The great mass of public records, especially the business records of government, is open to public access, and most meetings of most public bodies in North Carolina are conducted entirely in public.

Information about Private Citizens and Entities

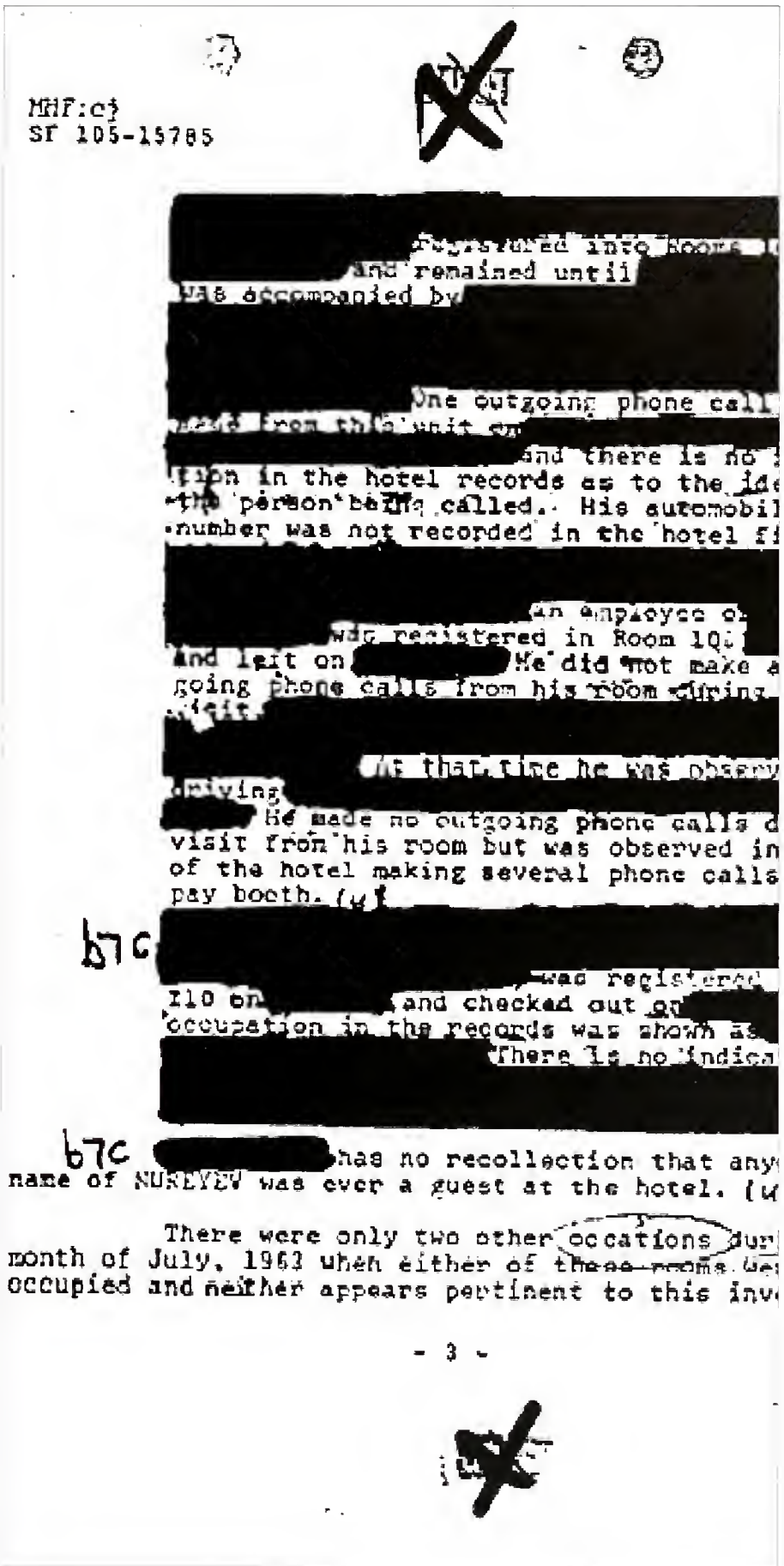
The broadest exceptions involve information that government holds about private citizens or entities, either because they deal with government or because government deals with them. These citizens and entities may pay taxes to government, receive special benefits from government, do business with government, be investigated by government, or otherwise interact with government. However the interaction takes place, the government acquires information about the private citizen or entity, and some of that information is likely to be considered personal or otherwise private by the citizen or the entity. Following are some important categories of private information held by government that are shielded by statute from public access or public meetings.

Tax information. Most of the information about taxpayers held by the North Carolina Department of Revenue is made confidential by statute, as is tax information held by local governments that reveals a taxpayer's income or gross receipts.[2] The confidentiality of tax information is particularly strong: improper release of the information is a crime, and the person responsible for the release must be terminated from public employment and may not hold a public job for five years.

These privacy policies, however, do not apply to most of the information held by local tax offices arising from administration of the property tax. Although a person's income is not public, the value of his or her house is.

Information about children and students. Information held by government about children is frequently excepted from public access. Further, federal law conditions federal aid to state and local education on the recipient's maintaining the confidentiality of student records. Accordingly, North Carolina law excepts student records from the public records act.[3] In addition, it excepts records of juveniles —both those enmeshed in the criminal justice system and those protected by social services agencies.[4]

Information about social services clients. Although the names of people receiving public assistance are public record, as is the amount they receive each month, all other information about them in the records of social services departments is confidential, and releasing the information in violation of



MHF:cj
SF 105-15785

[redacted] registered into Room [redacted] and remained until [redacted] was accompanied by [redacted]

One outgoing phone call [redacted] and there is no [redacted] tion in the hotel records as to the identity of the person being called. His automobile number was not recorded in the hotel [redacted]

[redacted] an employee of [redacted] was registered in Room 10[redacted] and left on [redacted]. He did not make any outgoing phone calls from his room during [redacted] visit.

At that time he was observed [redacted] driving [redacted]. He made no outgoing phone calls during visit from his room but was observed in the lobby of the hotel making several phone calls from a pay booth. (U)

b7C [redacted]

[redacted] was registered in Room 110 on [redacted] and checked out on [redacted]. Occupation in the records was shown as [redacted] There is no indication

b7C [redacted] has no recollection that any name of NURSEY was ever a guest at the hotel. (U)

There were only two other occations during month of July, 1963 when either of these rooms were occupied and neither appears pertinent to this inv

- 3 -

Citizens expect government records to be open to public view and not subject to undue censorship.

the statute is a misdemeanor.[5] This balance recognizes the public interest in monitoring social service programs but also refuses to force public assistance recipients to give up all claims of privacy as a condition of receiving aid.

Medical information. North Carolina law generally protects the confidentiality of medical records, and exceptions to the public records law extend confidentiality to medical records held by public hospitals, public health departments, mental health agencies, and other public health facilities.[6] (For more information on this topic, see the article on page 44.)

Records of library use. Public libraries are prohibited from releasing information that indicates what books library patrons have checked out or how they have otherwise used the library.[7]

Private telephone numbers. Most telephone numbers, of course, are listed in public telephone directories. Not only do people not consider their telephone number to be within their zone of privacy, but they wish it to be known. For various reasons, though, some numbers are considered private information and are unlisted. In at least two situations, state law protects the privacy of unlisted numbers. First, 911 centers normally seek the cooperation of telephone companies in obtaining all local telephone numbers for the 911 system. State law recognizes that some of the numbers provided by the telephone company may be unlisted and prohibits the release of any numbers received from the telephone company in this circumstance.[8] Second, a public employee's home telephone number is a part of the employee's personnel file that is not available to the public.

Information obtained in criminal investigations. State law excepts from the public records law most of the information gathered by law enforcement agencies in the course of criminal investigations.[9] A major reason for the exception is to protect the integrity of

an investigation; its subjects should not be privy to all its details.

But privacy considerations also shape this exception. First, the statute recognizes the privacy concerns of victims of crime and limits public access to their names and addresses, especially if a victim might be subject to harassment from suspects. Second, the statute recognizes that many suspects in a criminal investigation are ultimately cleared from suspicion. Apparently, legislators see no good purpose in disclosing that these people were ever suspects. Therefore, unlike criminal investigation records in some states, those in North Carolina do not become public once an investigation is completed; they are permanently shielded from public access.

Proprietary business information. Entities that wish to do business with a government agency often possess trade secrets integral to their business. As part of selecting the businesses with which they will deal, local governments and state agencies (as well as private businesses) often require their prospective business partners to reveal some of these secrets. Governments also may acquire business trade secrets through their regulation of businesses or business activities. The General Assembly has determined that a business should not have to relinquish its trade secrets in order to do business with state or local government, or because it is being regulated by government. So if a business reveals trade secrets to a local government or a state agency, that government or agency is prohibited from releasing the secrets.[10]

Information about Public Employees

As employers, local governments and state agencies maintain a wide variety of information about their employees, just as private employers do. A typical personnel file might include evaluations, letters of reference, personnel actions, results of drug and medical tests, a salary history, results of job tests, and records of internal investigations. For a private-sector employee, all this information is private. For a public employee, however, it is public unless excepted by statute from the public records law.

There are good arguments to be made for allowing public access to at least some of the information in a public employee's personnel file. Indeed, in a sense the public as a whole is the employer of a public employee and therefore might be thought entitled to the same rights of inspection of personnel files that private employers have. On the other hand, a private-sector employee's personnel files are not open to the stockholders of his or her company, even though they are the owners. Many public employees think that they should be entitled to the same privacy as private-sector employees.

The General Assembly has responded to these arguments by enacting a series of personnel privacy statutes that attempt to forge a balance between the public's interest in monitoring the performance of government and its employees, and the employees' interest in maintaining some privacy about their everyday work life.[11] The statutes make some information in a public employee's personnel file completely public, especially salary, the amount of the last salary change, and the nature and the date of the most recent personnel action affecting the employee. All else is excepted from automatic public access.

The statutes do, however, permit a number of more limited rights of access to or release of information from the files. Some are intended simply to facilitate the work of government itself—for example, a supervisor may see what is in an employee's personnel file, and the file's custodian may release most information in a file to an official of another government agency.

The treatment of attorney–client communications under the public records law is less protective of governmental clients. The state supreme court has held that the privilege itself does not automatically create an exception to the right of public access under the public records law.

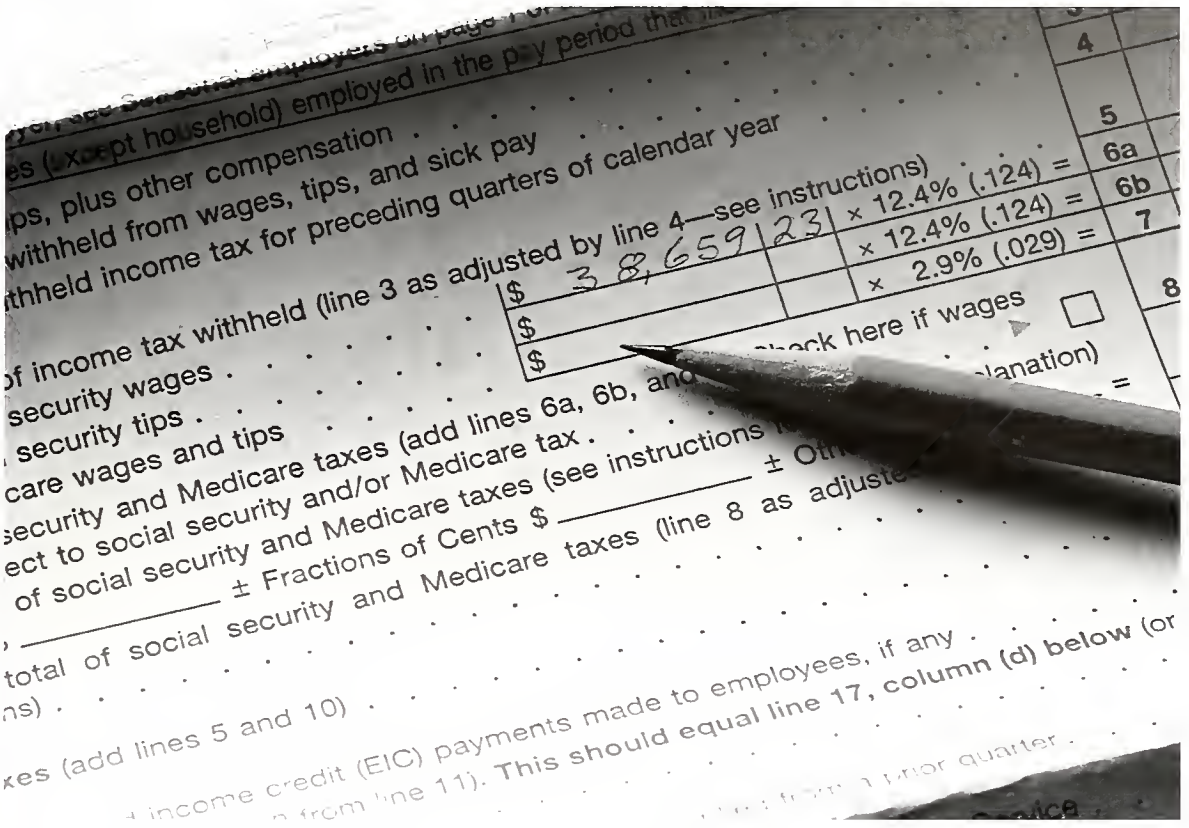
One of these limited rights of access is concerned with providing public information. The head of the appropriate agency or local government may release to the public information about a personnel action, including the reasons for the action, if doing so is "essential to maintaining the integrity" of the agency, "essential to maintaining public confidence" in the local government, or "essential to . . . maintaining the level or quality of services" provided by the agency or local government.[12]

The concerns for employees' privacy embodied in the personnel privacy statutes are repeated in an important exception to the open meetings law. That exception permits public bodies to hold closed sessions to consider the qualifications, the performance, and the fitness of a public employee or an applicant for employment, and to hear or investigate complaints by or against public employees.[13]

The Government's Own Privacy

A final set of exceptions to both the open meetings and the public records law recognizes that government agencies and local governments also have a need for privacy, or at least for secrecy. The policy considerations in this category of information, though, are clearly much more complicated than in either of the two preceding categories. Following are some examples of the protections.

Attorney–client confidentiality. A private individual or business entity is entitled to discuss legal matters in confidence with his, her, or its attorney, and to have written communications with the attorney also protected, even from being produced in a lawsuit. The considerations that underlie this policy also apply when the client is a govern-



North Carolina's public records law makes individuals' tax information confidential.

ment or a government agency, and that fact has been recognized, at least in part, by the General Assembly. One of the exceptions to the open meetings law permits a public body to meet in closed session with its attorney to discuss matters that are protected by the attorney–client privilege, and the statute expressly acknowledges that the privilege applies to government entities.[14]

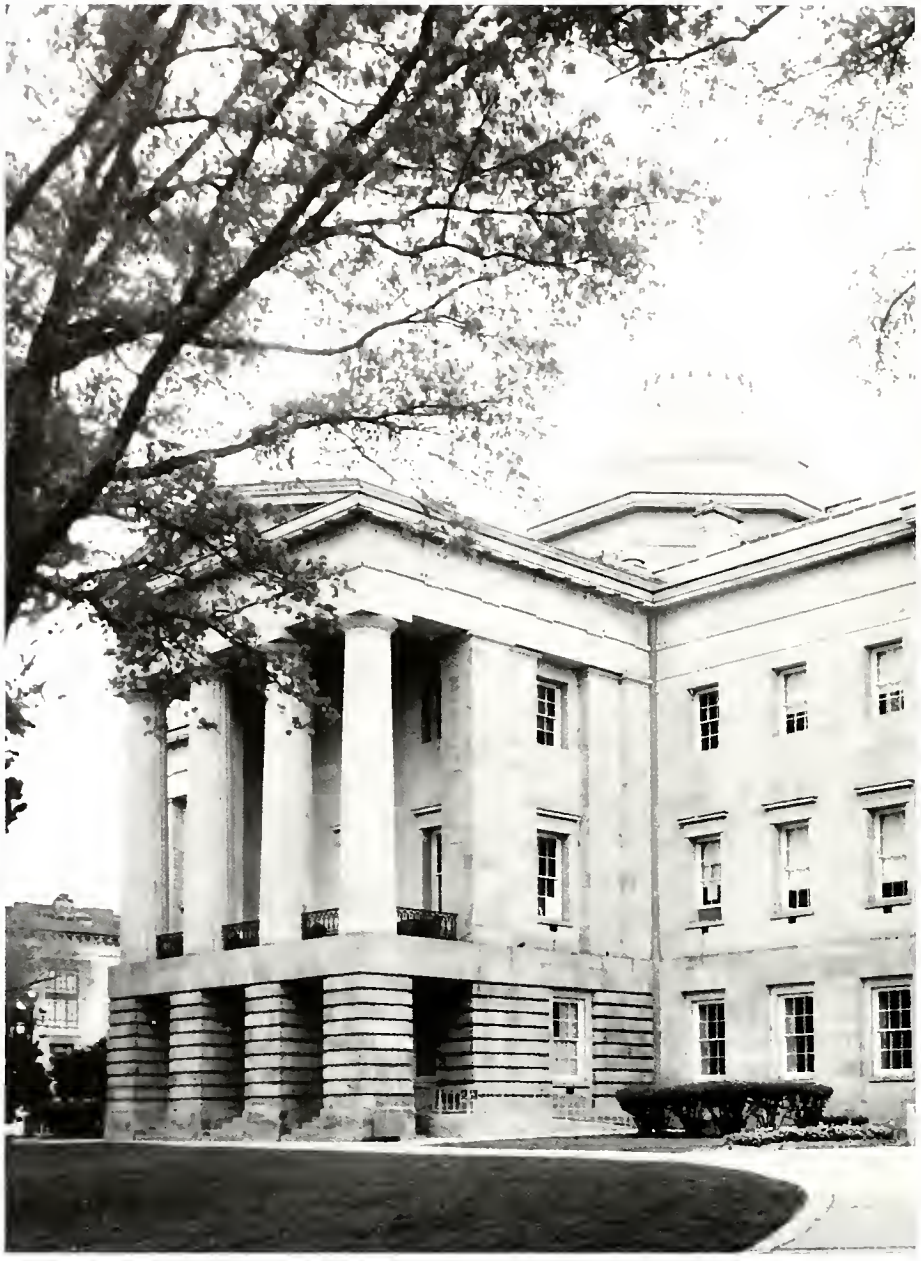
The treatment of attorney–client communications under the public records law, however, is less protective of governmental clients. The state supreme court has held that the privilege itself does not automatically create an exception to the right of public access under the public records law. Rather, the General Assembly must define the scope of the privilege for public records purposes.[15] The General Assembly has chosen to protect only one category of attorney–client communications—those from attorney to client respecting ongoing litigation.[16] The result is that many other communications between a public entity's attorney and the entity that would be privileged if made to a private citizen or entity are open to public access under the public records laws.

Adversarial situations. Like business organizations, governments are frequently involved in relationships that are somewhat adversarial. If the involved organizations were both private, each could develop its strategies without undue fear that the other party would become privy to them. When one of the organizations is a local government or a state agency, however, the demands of the open meetings or public records laws might force the governmental entity either to make its strategy in open meetings or make its strategy known to the other party through public records. The General Assembly has recognized this as a problem in select circumstances but not as a general principle and not in any patently consistent way. The exception in the open meetings law noted earlier, for attorney–client discussions, specifically mentions the need to have confidential discussions when the governmental client is involved in litigation. Similarly, another exception in the open meetings law permits a public body to hold a closed session when it is developing a negotiating position for the acquisition of real property.[17]

But other potentially adversarial situations are not protected by exceptions to the open meetings or public records laws. The open meetings law contains no exception when a government is *conveying* rather than acquiring property, no exception when it is acquiring (let alone conveying) *personal* property, and no exception when it is negotiating a contract not involving acquisition of real property. Similarly, even though the open meetings law permits lawmakers in a closed session to discuss developing a negotiating position for acquisition of real property, the public records law contains no exception that would protect any property appraisal the government may have had made as part of its negotiations.

Government as business competitor. Occasionally, governmental entities engage in activities in which they compete with private counterparts—for example, in health care, utility, cable television, and solid waste operations. Normally, business competitors keep a shroud of privacy over their operations, to maintain any competitive advantage they may have. Obviously, the general principles of the public records and open meetings laws conflict with business secrecy. Therefore the General Assembly

The long-standing policy of the North Carolina General Assembly is that the work of government be conducted in the open.



has permitted limited exceptions to protect government-operated businesses. One statute excepts from the public records law "information relating to competitive health care activities."[18] Another excepts discussions of proposed or existing contracts entered into by the state's joint power agencies (two entities through which cities with electric distribution systems helped finance nuclear power facilities).[19] These are the only instances, however, of the General Assembly's recognition of the special demands that competition might make on governments for privacy in their operations. No statute, for example, excepts from the public records law the competitive strategies of a city that distributes natural gas or a county that operates a facility for solid waste disposal.

Summary

The general policies of North Carolina law open up to public viewing and inspection the meetings and the records of state agencies and local governments. For the most part, these policies govern the day-to-day operations of government. The General Assembly has recognized, however, that sometimes the claims of privacy are strong enough to justify exceptions to these general policies. Most of the exceptions fall into three broad categories: information that government has received from or collected about individuals or private entities, and discussions about that information; information that government has received or created about governmental employees, and discussions about those employees; and situations in which the government itself has a strong need for privacy.

Notes

1. The public records law is centered in Chapter 132 of the NORTH CAROLINA GENERAL STATUTES (hereinafter G.S.), but exceptions to the right of public inspection are scattered throughout the General Statutes. The open meetings law is found in G.S. 143-318.9 through -318.18.

2. G.S. 105-259 for the N.C. Department of Revenue; G.S. 153A-148.1 for counties; G.S. 160A-208.1 for cities.

3. G.S. 115C-402. Other laws bar disclosure of information about students. See the article on page 36.

4. G.S. 7B-2901, -3000, -3001.

5. G.S. 108A-80.

6. G.S. 131E-97 (health care facilities); G.S. 130A-12 (public health departments); G.S. 122C-52 (mental health agencies); G.S. 143-518 (emergency medical services providers).

7. G.S. 125-19.

8. G.S. 132-1.5; G.S. 62A-9.

9. G.S. 132-1.4.

10. G.S. 132-1.2.

11. No single statute regulates the records of all public employees in North Carolina. Rather, several statutes apply to different kinds of governments. These statutes are broadly comparable, but, except for the city and county statutes, not identical. The principal statutes are G.S. 126-22 through -30 (state employees); G.S. 153A-98 (county employees); G.S. 160A-168 (city employees); and G.S. 115C-319 through -321 (public school employees).

12. The different statutes use slightly different criteria for justifying release of this information.

13. G.S. 143-318.11(a)(6).

14. G.S. 143-318.11(a)(3).

15. News and Observer Publ'g Co. v. Poole, 330 N.C. 465, 482–83, 412 S.E.2d 7, 17 (1992).

16. G.S. 132-1.1.

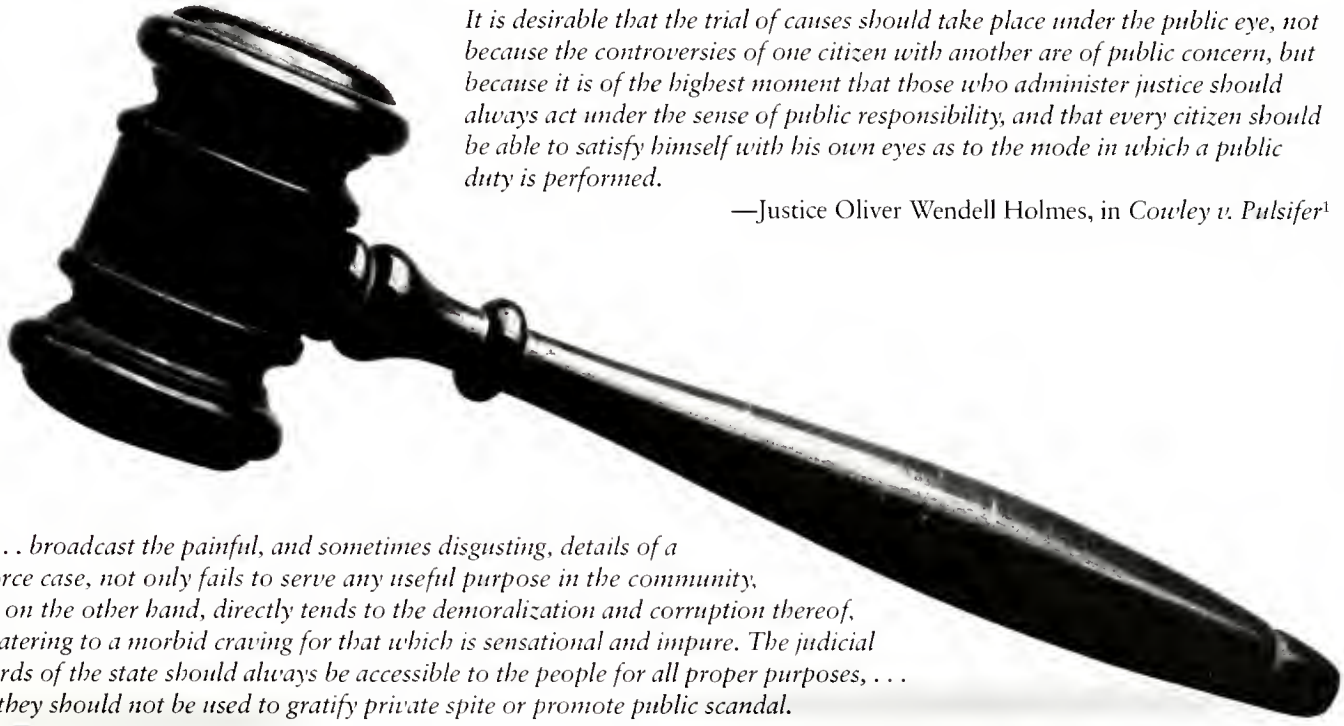
17. G.S. 143-318.11(a)(5).

18. G.S. 131E-97.3.

19. G.S. 159B-38.

Privacy and the Courts

James C. Drennan



It is desirable that the trial of causes should take place under the public eye, not because the controversies of one citizen with another are of public concern, but because it is of the highest moment that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed.

—Justice Oliver Wendell Holmes, in *Cowley v. Pulsifer*[1]

To . . . broadcast the painful, and sometimes disgusting, details of a divorce case, not only fails to serve any useful purpose in the community, but, on the other hand, directly tends to the demoralization and corruption thereof, by catering to a morbid craving for that which is sensational and impure. The judicial records of the state should always be accessible to the people for all proper purposes, . . . but they should not be used to gratify private spite or promote public scandal.

—*In re Caswell's Request*[2]

As these quotations demonstrate, courts have long been grappling with the tension between the privacy interests of people who use the courts and the public's interest in knowing what is going on in the courts. The tension persists today, although it sometimes takes twists and turns, as is evident in the debate over the use of potentially closed military courts in the aftermath of the terrorist attacks of September 11, 2001. The specifics of the issues that state courts face are different from those faced by the federal government in setting up military courts, but the fundamental tension between closing courts to protect a specific party's interest and opening them to serve the public's interest is similar. This article describes the ways in which North Carolina resolves those tensions in its courts.

In most instances the answer to the openness-or-privacy issue is that openness prevails. That is a cost of having a public court system. The following quote from the U.S. Supreme Court is fairly typical of courts' statements on the subject:

> *The right of access to criminal trials plays a particularly significant role in the functioning of the judicial process and the government as a whole. Public scrutiny of a criminal trial enhances the quality and safeguards the integrity of the factfinding process, with benefits to both the defendant and to society as a whole. Moreover, public access to the criminal trial fosters an appearance of fairness, thereby heightening public respect for the judicial process. And in the broadest terms, public access to criminal trials permits the public to participate in and serve as a check upon the judicial process—an essential component in our structure of self-government. In sum, the institutional value of the open criminal trial is recognized in both logic and experience.*[3]

Most courts and legislatures, when faced with the issue, find that justice, and society's pursuit of it, are too important to be performed away from the public's scrutiny. The real debate arises mostly when the information that

The author is an Institute of Government faculty member who specializes in court administration issues. Contact him at drennan@iogmail.iog.unc.edu.

is considered involves private, personal details of people's lives. Those details can include, among other things, the following:

- *Financial records.* For example, contests of wills may involve detailed discussions of a family's assets and liabilities, or a person's income often is introduced in evidence.
- *Testimony about intimate sexual matters or failed relationships with children or other family members.* For example, family law disputes often involve allegations of sexual dysfunction or marital infidelity, and sexual orientation or difficulties that children are having in school or in social settings frequently are at issue in custody cases.
- *Medical information.* For example, guardianship proceedings almost always involve detailed testimony and reports about the physical and mental condition of the person who is alleged to be incompetent. Also, nearly all claims for personal injury require evidence of the injury. Further, jurors often have to reveal publicly that they cannot hear or cannot sit for prolonged periods.
- *Sensitive business information.* For example, in a marital property dispute, the proceedings may reveal that a party's business is in financial trouble or reveal other information that a business owner would prefer remain confidential.

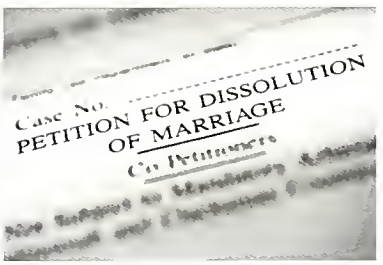
Such information is highly relevant, and the case cannot be disposed of fairly without it. That does not make its being disclosed any less embarrassing, and the disclosure is all the more unpleasant because it usually is compelled rather than volunteered.

One unfortunate consequence is that, when they can, people may avoid the courts to protect their privacy. But in many instances, avoidance is not an option. For example, a couple may not divorce except through the public courts, or people who are injured may find that litigation is their only recourse, even though they have to submit to personal questions about their private lives. In such instances, people may ask the courts or their legislators for help in preserving their privacy. The concern may be that of a litigant, a witness, a victim, or a juror.

This tension most often arises in relation to two rights of the public: the right to observe the proceedings and the right to look at the records later. The development of computer networks and large automated databases has generated the additional question of whether computer records are different from paper records. This article addresses each issue and then discusses the extent to which the privacy interests of a special category of court participants—jurors—are protected.

The Right to Attend Court Proceedings

The general rule is that court proceedings are open to the public. There are two kinds of exceptions to that rule: First, the presumption that the court will be open can be overridden in specific cases.[4] Second, in some instances the General Assembly has provided by statute that certain types of proceedings are either always closed to the public or may be closed by the judge.



A couple may not divorce except through the public courts, or people who are injured may find that litigation is their only recourse, even though they have to submit to personal questions about their private lives.

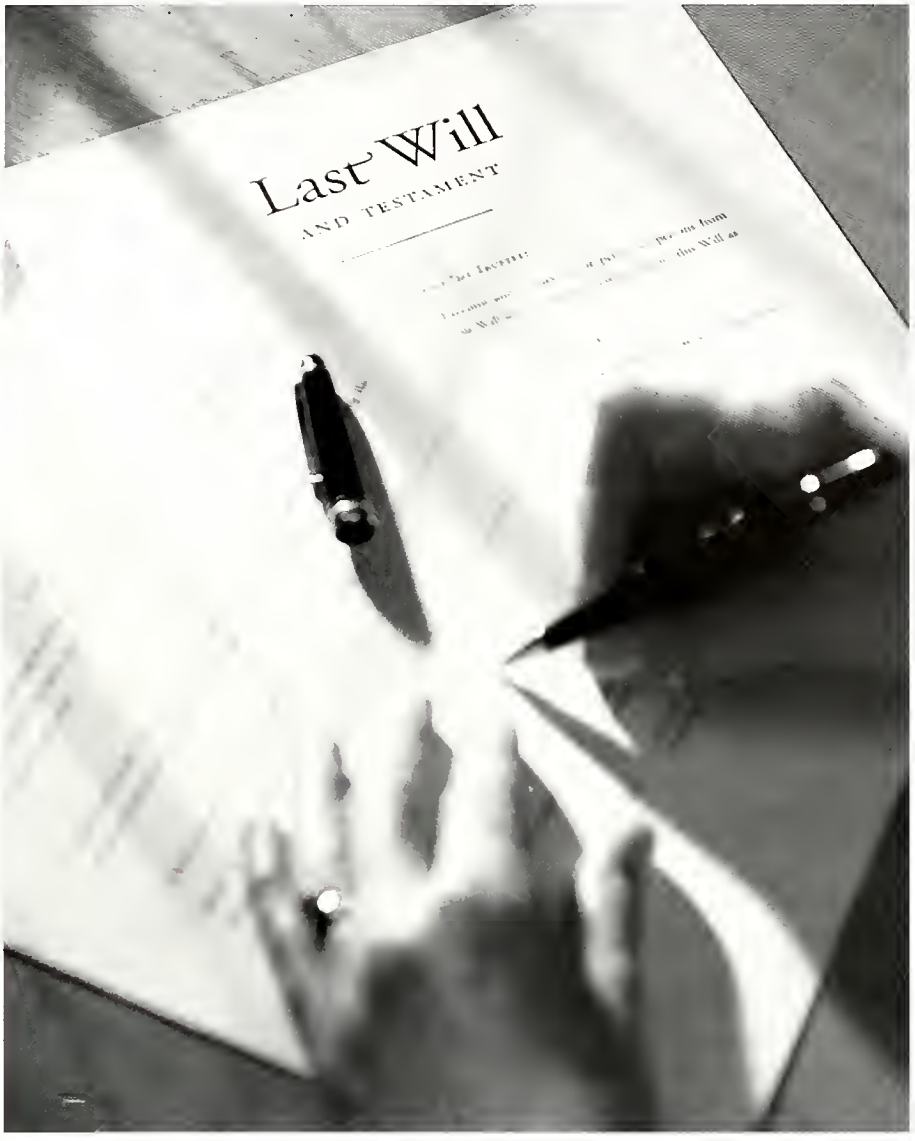
General Rule of Openness

The general presumption comes from Article I, Section 18, of the North Carolina Constitution, which provides that "[c]ourts shall be open; every person for an injury done him in his lands, goods, person, or reputation shall have remedy by due course of law; and right and justice shall be administered without favor, denial or delay." This provision was probably inserted to make it clear that courts were available to all people who needed to use them to resolve disputes, regardless of status.[5] However, the North Carolina courts have interpreted it also to mean that court proceedings are generally open to the public and the press. In the words of the North Carolina Supreme Court, "[T]he open courts provision of [the N.C. Constitution] guarantees a qualified right on the part of the public to attend civil court proceedings."[6]

A similar right applies in criminal cases.[7] The U.S. Supreme Court has held that the First Amendment rights to freedom of speech and freedom of the press contain an implicit, qualified right of the public to attend criminal trials.[8] However, both the North Carolina Supreme Court and the U.S. Supreme Court have ruled that the right is not absolute. In criminal cases the U.S. Supreme Court has indicated that the right to attend is significant. To limit that right in order to prevent the disclosure of sensitive information, the government must demonstrate that a closing of the court is necessary to serve a compelling governmental interest; that the closing is narrowly tailored to serve that interest; and that there is no reasonable alternative to the closing.[9]

North Carolina's courts apply a similar standard in determining if civil proceedings may be closed.[10] If a court determines that they should be closed, it must make specific findings to support its decision. That is a difficult standard for anyone seeking closure to meet, and as a result, closing of civil proceedings is not common in North Carolina.[11]

In the situations in which courts have been closed to the public, privacy is not always the interest asserted. For example, the North Carolina Supreme Court has ruled that court reviews of medical peer reviews of doctors to determine their fitness to practice in a hospital may be conducted in closed court hearings, to preserve the public's interest in "effective, frank, and uninhibited exchange among medical peer review members."[12] That kind of exchange is necessary to preserve the quality of health care delivered by



Court cases involving contests of wills may delve deeply into private financial information.

doctors. Therefore, opening the hearing would compromise the ability of peer review agencies to gather full and complete information. Although closing the court protects the privacy of the doctor under review, protection of his or her privacy is not the justification for the closing.

Similarly, when criminal proceedings are closed to the public, a common reason cited is that extensive press coverage threatens the defendant's ability to get a fair trial. That concern is greatest at early stages of the proceeding, such as in a preliminary hearing or in jury selection.[13] Thus, although a disclosure of information may be embarrassing or otherwise involve a loss of privacy by the party affected, it is not often the basis for a court to close proceedings in North Carolina. No appellate cases or legislative actions in this state allow embarrassment alone to support the closing of a court proceeding.

Statutory Exceptions

In the following instances, the General Assembly has enacted statutes providing that court proceedings not be open to the public. In most of these cases, the privacy interest being protected is that of either a person testifying or a person who is a party to the action.

- *Juvenile cases.* G.S. 7B-2402 provides that cases involving the juvenile code[14] are open to the public "unless the court closes the hearing or part of the hearing for good cause." If the hearing is closed, the court may allow any person directly involved in the proceeding to attend. A juvenile may ask that the hearing be open, and the court must honor that request. Juvenile matters have historically been closed to the public, but the trend is toward open hearings.
- *Involuntary commitments.* G.S. 122C-267(f) provides that hearings to determine if a person should be or remain involuntarily committed to a state mental health facility are closed to the public unless the person requests that the hearing be open. This statute was enacted in 1985; commitment hearings had not been closed before that.
- *Adoptions.* G.S. 48-2-203 provides that any judicial hearing in an adoption be conducted in closed court.
- *Judicial consent for a minor's abortion.* North Carolina requires that if a pregnant girl under age eighteen is seeking an abortion, she must obtain the consent of a parent. If she does not want to seek a parent's consent, G.S. 90-21.8 allows her to apply to a district judge for a waiver of parental consent. That proceeding is confidential and is to be conducted in such a manner that the girl's identity is kept confidential throughout the process, including any appeals.[15]
- *Testimony of a victim of a sexual offense.* G.S. 15-166 allows trial judges to "exclude from the courtroom all persons except the officers of the court, the defendant, and those engaged in the trial of the case" when a victim in a rape or sexual offense case is testifying.

The extent to which the proceedings are closed under these exceptions is a function of the privacy interest to be protected. When the party to be protected is not on trial—for example, a rape victim—the protection is narrowly drafted to shield only the victim's testimony. When the party to be protected is on trial in some fashion, the entire proceeding is shielded from public view.

Perhaps the most striking feature of the list of exceptions is how short it is. The range of embarrassing matters that

can be covered in court is remarkably broad, but the legislature has provided only five exceptions.

Access by Media

To emphasize the importance of public access to the courts, the General Assembly also has enacted a statute making it clear that the news media may publish any report they see fit on any matter that occurs in open court, and that any attempt by a court to prohibit anyone from publishing a report about anything that occurs in open court is "null and void, and of no effect."[16] That statute is consistent with U.S. Supreme Court decisions holding that the truthful publication of facts obtained from courts may not be punished.[17] North Carolina law also provides that no person may be held in contempt of court for the content of any broadcast or publication unless the dissemination presents "a clear and present danger of imminent and serious threat to the administration of criminal justice."[18]

In addition, the news media may assert their right to attend court proceedings (or to review the records of a case) by filing a motion in the case.[19] The statute granting this privilege was enacted in the 2001 session of the North Carolina General Assembly. It effectively reversed a North Carolina Supreme Court decision that news organizations had to file a separate lawsuit seeking access.[20] News organizations complained that doing so would take time and that the trial in which the issue of access arose would be over before the issue could be raised.

Although the public has a right to attend court proceedings, relatively few members of the public actually do attend them. Most people learn what they know about courts from the news media. Courts treat newspaper and other reporters in the same way that they treat other members of the public. Different rules apply to television and photographic coverage, however.

Television coverage and photographic coverage have the potential to reach many more people than can attend a proceeding in person, and they can do so visually, revealing a person's identity more effectively. Courts have historically been reluctant to allow televising or photographing of court proceedings because they have feared that a camera's presence would turn the trial into a search for publicity instead of for justice.

The U.S. Supreme Court has not found that the right of the public to attend court proceedings includes the right to televise or photograph them.[21] As a result, the issue is left to the states to decide. Many states have either denied access or restricted it. North Carolina law on this matter was established in a rule adopted by the North Carolina Supreme Court.[22] It presumes that television coverage and still photography of most court proceedings should be allowed but gives the presiding judge the discretion to prohibit them. The court established some exceptions for circumstances in which it felt that no such coverage should be allowed:

- Adoptions, juvenile cases, and custody, divorce, and alimony actions
- Cases involving evidence of trade secrets
- Testimony of minors and victims of sex crimes
- Jurors generally

The news media may publish any report they see fit on any matter that occurs in open court, and . . . any attempt by a court to prohibit anyone from publishing a report about anything that occurs in open court is "null and void, and of no effect."

Court Records

General Rule of Openness

Review of court records affects privacy differently than open court proceedings do. Written records are permanent. They may contain only summary information about a criminal or civil trial or proceeding, but that record, if it is public, may be reviewed long after the event has taken place. If a person is convicted of a drug offense at age eighteen, he or she is not likely to feel the same degree of embarrassment at the time of conviction that he or she will feel at age thirty or sixty. Permanent public records make it possible to find out about such convictions long after they have faded from the memories of most people.

As is true with court closings, the general rule about court records is that they are open to public inspection. In addition to the general public records statute, there is a specific statute making the court records maintained by the clerk of court (the official records) open for inspection.[23] Also, North Carolina appellate courts have made it clear that the records held by the courts are public.[24]

Civil Cases

There are statutory exceptions. Records of closed court proceedings are usually closed.[25] In some civil cases, to protect a party or a witness from unreasonable annoyance, embarrassment, oppression, or undue burden or expense, the court may provide that depositions (the testimony of a witness taken in advance of a trial to discover evidence in the case) may be sealed and opened only with the approval of the court.[26]

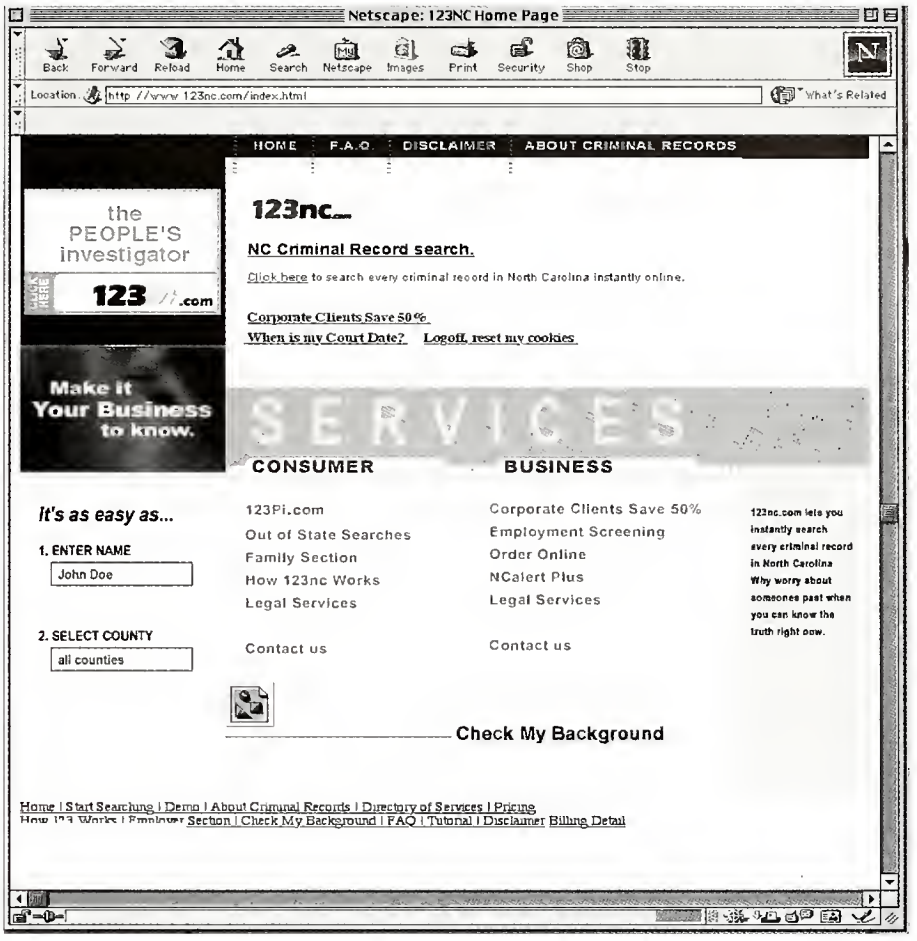
Criminal Cases

There also are instances in criminal courts in which records are not made available to the public. When a criminal defendant's competency to stand trial is questioned, the reports of the medical personnel conducting the examination are sealed, and they become public records only if the reports are introduced into evidence.[27] Also, presentence reports are not public records; only court officials with a need to see them may do so.[28] Similarly, material prepared by sentencing-services programs may be withheld from public inspection.[29]

Exceptional Cases

Judges often are asked to seal court records in a specific case. In *Virmani v. Presbyterian Health Services Corpora-*

A private company that has contracted with North Carolina's Administrative Office of the Courts makes the state's criminal records available on-line for a fee.



tion, the North Carolina Supreme Court approved the sealing of various hospital records used as part of a court review of a physician's fitness to serve at a hospital, in part on the basis of the legislature's indication that such records should be confidential. The court held that, notwithstanding public records or related statutes, trial courts have the

> *necessary inherent power granted them by Article IV, Section I of the North Carolina Constitution to control their proceedings and records in order to ensure that each side has a fair and impartial trial. . . . A trial court may, in the proper circumstances, shield portions of court proceedings and records from the public; the power to do so is a power rightly pertaining to the judiciary as a separate branch of the Government, and the General Assembly has "no power" to diminish it in any manner.*[30]

That language also could apply to records not classified by the legislature as confidential. The North Carolina Supreme Court instructed lower courts to use the power sparingly and only when necessary for the fair administration of justice, or "where for reasons of public policy, the openness ordinarily required of our government will be more harmful than beneficial."[31] A court exercising the power must first consider any alternatives to closure and then specify in writing the facts that support its decision. As is the case with motions to close court proceedings, the burden on the party seeking closure is high, and court records are rarely sealed.

Settlements

In practice, one important exception to the general rule of openness is in civil cases settled before trial. In settlement negotiations it is not unusual for one party to ask that the terms of the settlement be sealed and that such a provision be in the final settlement.

The General Assembly has provided that settlement documents in lawsuits against governmental agencies, except for malpractice actions against hospitals, may not be sealed unless the court determines that the presumption of openness is overcome by an overriding interest in maintaining the confidentiality of the proceeding and that the interest may not be served by any measure other than sealing the documents.[32] The statute states a preference that such records be open, however.

In nongovernmental civil cases, there is no such requirement, and the general authority described in *Virmani* applies. Unless the court exercises that authority, the public records law applies to the records of the case. Defendants involved in multiple lawsuits often seek closure to keep the terms of one settlement from affecting other cases. Sealing of settlements is controversial, as this excerpt from a legal manual prepared for news media personnel notes:

> *This trend [to seal settlements] is opposed by . . . news organizations because the sealing of court documents allows the public courts to be turned into private dispute resolution forums. The effect is to keep from the public information that could help citizens, such as settlements for injuries stemming from the use of defective or dangerous products.*[33]

Computer Records

The official record of any court proceeding is the paper record in the file of the case, maintained in the office of the clerk of court. That has implications for the ease of use of the record. For example, if a researcher wanted to do a systematic review of results in impaired driving cases, using the case files would require looking at hundreds of thousands of case files in 100 counties. It is not surprising that projects like that are seldom done using the original, or "source" documents, even though the results would be of great interest to the public. Similarly, looking at a person's criminal history or the number of civil judgments rendered against him or her would be an insurmountably difficult

task if the research had to be conducted in 100 courthouses. Even if the search is for a single record—a person's record of being sued in one county, or his or her history of impaired driving in a county—the search must be conducted in the courthouse, during regular business hours. This often is not the most convenient place or time for the search to occur.

Computers can change that—and they have. Much of the important information that is found in source documents for North Carolina's courts also is maintained in a database on the state court system's mainframe computer. This database often is referred to as "compiled records." Although access to the database is easier in some ways—it can potentially be gained anytime, anywhere—it may be more difficult in other ways because navigating a computer-based record system often requires specialized knowledge about that system.

The emergence of compiled records raises the important question of whether they should be treated in the same way as source records. In other contexts, governments have recognized that they are different. The best example is state criminal histories. In each state a central, automated repository of such information is available to all law enforcement personnel. All the information in the repository has been obtained from public records, but it is not available to the public.[34] In weighing the risk of harm from widespread dissemination of criminal records against the benefits to the public, Congress opted in favor of restricting access.

As state court systems develop more powerful, centralized databases, they face the same issues. The report of a study by the Conference of State Court Administrators (composed of the chief executive officers of the fifty state court systems) suggests that compiled records be treated in the same way as source records, and be equally available. The report recognizes, however, that there may be instances in which the content of the record should not be made public in either the source document or any compiled documents.[35]

North Carolina's statutes follow that policy.[36] There is no statutory prohibition on dissemination of the court system's compiled records. Thus the compiled records, like the source records from which they come, are public.[37] Records that are shielded from public inspection in their original form are not available in electronic formats. A person requesting a copy of public records "may elect to obtain them in any media in which the public agency is capable of providing them."[38]

Much of the important information that is found in source documents for North Carolina's courts also is maintained in a database on the state court system's mainframe computer. This database often is referred to as "compiled records."

Another way in which compiled electronic records differ from source records is that they also may be obtained from private businesses. The Administrative Office of the Courts has contracts with some private agencies giving them access to the state database and allowing them to resell the records. The records can be purchased by anyone and are available on the Internet.[39] The Administrative Office of the Courts retains the funds generated by these contracts to support its technology programs.[40]

Juror Privacy Issues

Jurors are a vital part of the court system. Although relatively few cases are disposed of by jury trials, the fact that a jury is available is very important. All participants in civil settlement or criminal plea negotiations consider what a jury would do in making judgments about the reasonableness of an offer from the other side. In a real sense, juries determine what justice means in a community.

Jurors are not paid well, are forced to miss work, and in many instances do not have particularly good physical surroundings in which to do their job.[41] Nevertheless, every year, tens of thousands of citizens report to courthouses for jury service, most of them cheerfully. As they begin their service, tension between their desire for privacy and the need for open information about the courts once again arises. As is true in other contexts, the privacy interest rarely prevails.

The issue can come up in a variety of contexts. In rare, high-profile cases, a juror's lifestyle may be investigated before he or she reports for jury service. When the juror reports for duty and is questioned about his or her fitness to serve, the questioning (called *voir dire*) often delves into personal matters as attorneys determine if potential jurors have fixed opinions on issues important to the case. If a juror completes a questionnaire with personal information, he or she may be concerned about the retention of that document. If a trial is highly publicized, a juror may be the subject of publicity. Also, to protect either their privacy or their safety, jurors may have concerns about the parties to the case knowing their address.

Data are available on how North Carolina jurors feel about some of those issues. In a recent survey, 43 percent of North Carolina jurors responding felt that *voir dire* questions were unnecessary, 27 percent said the questions made them uncomfortable, and 27 percent considered the questions invasions of their privacy. One of the most frequently raised concerns was the embarrassment of having to discuss prior criminal convictions publicly. Further, 25 percent of those surveyed felt that unnecessary questions were asked about their families, their employment, their church affiliation, and like matters.

Jurors' main concern was that such questions often had the effect of stereotyping them based on where they lived, worked, or worshipped. Of those asked about their religion, 20 percent thought the questions were irrelevant and intrusive.

In general, the survey found that

jurors' interests in privacy had several components. Jurors wanted to limit public disclosure of sensitive or embarrassing information. They did not want the questions to cause them to have concerns about their personal safety. Also, they wanted the questioning to minimize the possibility of their being stereotyped.[42]

The American Bar Association's standard, a benchmark against which courts measure their systems, provides that "the Judge should ensure that the privacy of prospective jurors is reasonably protected and that questioning is consistent with the purpose of the voir dire process."

If protecting jurors' privacy was the dominant value in the judicial system, the practices just mentioned would not be permitted. The system exists, however, to provide parties with a fair trial, in which they are judged by their peers and not by an agent of the government. That system has costs, and one of them is some loss of a juror's interest in his or her privacy.

Within that framework, though, jurors have limited protections. The American Bar Association's standard, a benchmark against which courts measure their systems, provides that "the Judge should ensure that the privacy of prospective jurors is reasonably protected and that questioning is consistent with the purpose of the voir dire process."[43]

In North Carolina, some statutes and policies help serve that interest. First, the master jury list for each county is available for public inspection, but it does not list jurors in the order in which they will be summoned.[44] This makes it less likely that potential jurors will be the subject of an investigation before being called to serve.[45]

Second, in instances in which material is appropriate for voir dire questioning but is nonetheless embarrassing or highly sensitive, the U.S. Supreme Court has approved the closing of the courtroom to the public during jury selection. The Court allowed the closing when the process involved questions that "touch on deeply personal matters that the person has legitimate reasons for keeping out of the public domain." To close the court in those instances, the Court directed trial judges to

> *maintain control of . . . jury selection and [to] inform the array of prospective jurors, once the general nature of sensitive questions is made known to them, that those individuals believing that public questioning will prove damaging because of embarrassment, may properly request an opportunity to present the problem to the judge in camera [in private], but with the counsel present and on the record.*[46]

Finally, judges may limit the scope of questions allowed in *voir dire* to prevent questioning on inappropriate matters. In the case establishing that authority most clearly, the trial judge prohibited the defense attorney in a death-penalty case from inquiring into a juror's religious denomination or participation in church activities: "Even though the state and the defendant are entitled to inquire into a prospective juror's beliefs and attitudes, neither has the right to delve without restraint into all matters concerning potential jurors' private lives."[47]

Conclusion

The job of courts is to balance interests to determine just results in specific cases. They also must strike the right balance when privacy interests conflict with other important interests, such as the public's right of access to its courts or a party's right to a fair trial. In most cases the privacy interest, although important, does not prevail because, in a democratic society, having a justice system in which citizens have confidence is so important that citizens are willing to give up some of their privacy. The balance has changed over the years and will continue to do so, but the goal is likely to remain the same: to keep the courts as a public institution that has the confidence of the public and does not unduly invade the privacy of those who use it.

Notes

1. Cowley v. Pulsifer, 137 Mass. 392, 395 (1884).

2. *In re* Caswell's Request, 18 R.I. 835, 835, 29 A. 259, 259 (1893).

3. Globe Newspaper Co. v. Superior Ct. for Norfolk County, 457 U.S. 596, 606 (1982).

4. In this article, when I refer to closing the courts, I mean restricting the access of the press and the public to the proceedings. Court personnel, witnesses, parties, attorneys, and others with a specific reason to be present may be in the courtroom. Other situations in which courtrooms are not fully open to all parties, such as "sequestration" (seclusion) of witnesses [N.C. GEN. STAT. § 15A-1225 (hereinafter G.S.)], extraordinary security measures that impose restrictions on courtroom access [G.S. 15A-1034], and special arrangements to allow child victims to testify by closed-circuit television [*see In re* Stradford, 119 N.C. App. 654, 460 S.E.2d 173 (1995), are beyond the scope of this article. Moreover, they do not directly affect the privacy interests of the people testifying, since members of the public may attend the testimony.

5. JOHN V. ORTH, THE NORTH CAROLINA STATE CONSTITUTION, WITH HISTORY AND COMMENTARY 53–55 (Chapel Hill, N.C.: Univ. of N.C. Press, 1993). Orth notes that the language was derived from the Magna Carta. *See also* Louis F. Hubener, *Rights of Privacy in Open Courts—Do They Exist?*, 2 EMERGING ISSUES IN STATE CONSTITUTIONAL LAW 189 (1989).

6. Virmani v. Presbyterian Health Services Corp., 350 N.C. 449, 476, 515 S.E.2d 675, 695 (1999).

7. *See* State v. Burney, 302 N.C. 529, 537–38, 276 S.E.2d 693, 698 (1981); *In re* Nowell, 293 N.C. 235, 249, 237 S.E.2d 246, 255 (1977); *In re* Edens, 290 N.C. 299, 306, 226 S.E.2d 5, 9–10 (1976).

8. *Globe Newspaper*, 457 U.S. at 603–07. The Court has since ruled that the right extends to jury selection proceedings, Press Enter. Co. v. Superior Ct. of Cal., Riverside County, 464 U.S. 501 (1984), and to preliminary hearings conducted by a magistrate, El Vocero de Puerto Rico v. Puerto Rico, 508 U.S. 147 (1993).

9. *Globe Newspaper*, 457 U.S. at 606.

10. *Virmani*, 350 N.C. at 476–78, 515 S.E.2d at 693–95.

11. As one commentator notes, the burden is so high that the right of access is "close to absolute in practice." Karen Rhodes, *Open Court Proceedings and Privacy Law: Re-Examining the Bases for the Privilege*, 74 Texas Law Review 881, 908 (1996). *See also* Hall v. Post, 323 N.C. 259, 372 S.E.2d 711 (1988), in which the North Carolina Supreme Court held that there is no tort liability for invasions of privacy by the publication of true but private facts.

12. *Virmani*, 350 N.C. at 478, 515 S.E.2d at 694.

13. If there is concern about a jury's ability to handle publicity during a trial, the trial judge may "sequester" (seclude) the jury. G.S. 9-17, 15A-1236. Sequestration is rarely used in North Carolina; judges instead give jurors specific instructions to avoid any publicity about the trial. *See* North Carolina Pattern Jury Instructions for Criminal Cases § 100.31 (N.C. Super. Ct. Judges Conference, Committee on Pattern Jury Instructions, June 1978).

14. The types of cases include allegations of child abuse, neglect, or dependency, or of juvenile delinquency.

15. This is the only instance in which the statutes authorize litigants to file an action without using their name. In some other states and in federal courts, judges may allow litigants to proceed anonymously (as John Doe or Jane Roe). *See* 1 Gray Wilson, North Carolina Civil Procedure 173 (2d ed., Charlottesville, Va.: Michie, 1995). Whether the practice would be approved by North Carolina's appellate courts is unclear, but in courts where the practice is authorized, the court must weigh the privacy interest of the party against the interest of the public in having access to court information. Typically the cases in which the party is allowed to proceed anonymously involve issues like birth control, abortion, sexual orientation, child custody, or challenges to religious observances. Doe v. Diocese Corp., 43 Conn. Supp. 152, 647 A.2d 1067 (1994).

16. G.S. 7A-276.1.

17. Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).

18. G.S. 5A-11(b).

19. G.S. 1-72.1.

20. Virmani v. Presbyterian Health Services Corp., 350 N.C. 449, 515 S.E.2d 675 (1999).

21. For a discussion of the history of the courts' handling of this issue, *see* Cathy Packer & Hugh Stevens, North Carolina Media Law Handbook, 7–10 (Chapel Hill, N.C.: N.C. Press Found., 1996).

22. General Rules of Practice for the Superior and District Courts Rule 15, Electronic Media and Still Photography Coverage of Public Judicial Proceedings (Charlottesville, Va.: LEXIS Publ'g Co., 2001).

23. For a discussion of the general public records statute in relation to privacy interests, see the article on page 20. The specific statute pertaining to the court records maintained by the clerk of court is G.S. 7A-109(a), which provides, "Except as prohibited by law, [clerk of court] records shall be open to the inspection of the public during regular office hours, and shall include civil actions, special proceedings, estates, criminal actions, juvenile actions, minutes of the court, judgments, liens, lis pendens, and all other records required by law to be maintained."

24. *Virmani*, 350 N.C. 449, 515 S.E.2d 675. *See* Times-News Publ'g Co. v. State of N.C., 124 N.C. App. 175, 476 S.E.2d 450 (1996); News and Observer Publ'g Co. v. Poole, 330 N.C. 465, 412 S.E.2d 7 (1992).

25. Juvenile records and involuntary commitment records are confidential unless ordered to be opened by the court. G.S. 7B-2900, -3000; G.S. 122C-207. All records of minors seeking waivers of parental consent for abortion are confidential. G.S. 90-21.8. All adoption records of the court that could lead to the identity of the birth parents are to be sealed, unless ordered to be opened by a court. G.S. 48-9-102.

26. G.S. 1A-1, Rule 26(c). The court also may limit the matters into which the discovery proceeding may inquire, or prohibit the discovery altogether.

27. G.S. 15A-1002(d).

28. G.S. 15A-1333.

29. *Id.*; G.S. 7A-773.1, -774. Sentencing-services programs provide information to the court and to attorneys in criminal cases about possible sentences for offenders that do not involve commitment to prison. The information is similar to the kind of information that is contained in presentence reports but often is more comprehensive and detailed, especially with respect to the defendant's social and medical history.

30. Virmani v. Presbyterian Health Services Corp., 350 N.C. 449, 476, 463, 515 S.E.2d 675, 695, 685 (1999).

31. *Id.*, 350 N.C. at 463, 515 S.E.2d at 685.

32. G.S. 132-1.3.

33. Packer & Stevens, North Carolina Media Law Handbook, at 17.

34. Pub. L. No. 92-544, 86 Stat. 1115. *See also* 28 U.S.C. § 534. For a discussion of the information contained in this database, *see* James C. Drennan, *Obtaining Record Checks to Reduce Risk*, Popular Government, Winter 1999, at 30.

35. Conference of State Court Administrators, Concept Paper on Access to Court Records (Aug. 2000). A Model Policy on Public Access to Court Records is being drafted by the National Center for State Courts (Williamsburg, Va.). It is being prepared on behalf of the Conference of State Court Administrators and the Conference of Chief Justices. The initial draft is available at www.courtaccess.org/modelpolicy (last modified Mar. 11, 2002).

36. Courts in some other jurisdictions protect more records from public inspection than North Carolina courts do. Federal bankruptcy courts prevent access to Social Security numbers contained in electronic filings in those courts. Arizona and New York state courts make all electronically stored information about domestic case files confidential except the final orders of divorce, custody, property distribution, or child support. Privacy and Public Access to Court Records, Memorandum from Pamela Best, Associate Counsel, N.C. Admin. Office of the Courts, to Judge Robert Hobgood, Director, N.C. Admin. Office of the Courts (Nov. 27, 2001) (on file with Best and with author).

37. G.S. 132-1: "Public records . . . shall mean all . . . electronic data processing records, . . . made or received pursuant to law or ordinance in connection with the transaction of public business. . . ."

38. G.S. 132-6.2.

39. G.S. 7A-109(d) provides authority for the Administrative Office of the Courts to charge for such access, and that office currently has contracts with several private agencies.

40. G.S. 7A-343.2.

41. G.S. 7A-312 establishes a fee of $12 per day to be paid to jurors for the first five days of jury service, $20 per day for additional days. For a summary of the results of a survey conducted by the Administrative Office of the Courts, *see* Miriam S. Saxon, *The Verdict Is In: Citizens' Views on Jury Service*, Popular Government, Spring 1999, at 29.

42. Mary Rose, *No Right to Remain Silent: Privacy and Jurors' Views of the* Voir Dire *Process* (forthcoming in Judicature), Paper presented at Jury Summit 2001, Feb. 2, 2001, New York (New York State Unified Court System and National Center for State Courts). The survey involved jurors who participated in thirteen criminal trials; 67 percent completed the survey. Surveys from other states are consistent.

43. Standards Relating to Jury Use and Management Standard 7(c) (1993).

44. The master list is the list of all jurors who may be summoned in each two-year cycle for which the list is prepared.

45. G.S. 9-4, -2.1. For a discussion of the juror's right to privacy in this situation, *see* David Weinstein, *Protecting a Juror's Right to Privacy: Constitutional Constraints and Policy Options*, 70 Temple Law Review 1 (1997).

46. Press Enter. Co. v. Superior Ct. of Cal., Riverside County, 464 U.S. 501, 511, 511 (1984).

47. State v. Lloyd, 321 N.C. 301, 307, 366 S.E.2d 316, 321 (1988).

Employee Privacy and Workplace Searches

Stephen Allred

Public employers routinely furnish employees with offices, desks, file cabinets, lockers, computers, and other items with which to perform their jobs. Even though the employer pays for these items, the employees who use them take on a sense of ownership —and privacy—in their workspaces. Indeed, given the amount of time people spend at the workplace these days, the office often becomes a home away from home, complete with pictures of the family, souvenirs from trips, and a large collection of coffee cups.

But what happens when a public employer has reason to suspect that an employee has engaged in inappropriate activity, and the employer wants to search the employee's workplace? May a supervisor root around in an employee's desk in hopes of finding proof of misconduct? May an employer search an employee's computer, even if it is password protected? Many do so, according to a recent survey conducted by the Society for Human Resource Management.[1] Sixty-two percent of responding employers said that they sometimes monitored Internet use, 58 percent e-mail, and 42 percent telephone calls. This article explores the current state of the law on employee privacy and workplace searches. The discussion pertains strictly to public employers and employees. Generally the law does not protect private-sector employees from workplace searches by their employers.

High Court Recognition of Public Employee Privacy Interest

For the Fourth Amendment to protect any individual from government searches, the government must cross a judicially constructed threshold. In *Katz v. United States*, the U.S. Supreme Court held that Fourth Amendment protections are triggered only if a person has a reasonable expectation of privacy.[2]

For this standard to be met, the person must have "an actual or subjective expectation of privacy" in the area or the things to be searched and this expectation must "be one that society is prepared to recognize as 'reasonable.'"[3] If a person does not have an expectation of privacy that is recognized as reasonable, the Fourth Amendment is not triggered, and the government may search at will. It may search without a warrant and even without the most rudimentary showing of "reasonable suspicion"—that is, grounds to believe that the person has engaged in illegal or inappropriate conduct. (For a fuller discussion of *Katz* and the requirements of the Fourth Amendment, see the article on page 13.)

The notion that public employees may have a protected privacy interest in their workplace is a relatively recent development in the law. In 1987, for the first time, the U.S. Supreme Court

The author is an Institute of Government faculty member who specializes in employment law. He is currently on leave from the Institute to serve as an associate provost at UNC–Chapel Hill. Contact him at steve_allred@unc.edu.

considered whether the Fourth Amendment protected public employees from searches of their workplaces. In *O'Connor v. Ortega*, a physician who worked in a state hospital was suspected of various acts of misconduct, including theft of hospital property and sexual harassment.[4] The executive director of the hospital suspended the physician pending completion of an investigation into the alleged misconduct. As part of that investigation, the executive director and other management officials entered the physician's office and searched his file cabinets and desk. Certain materials found in that search were used in the subsequent administrative proceeding to remove the physician.

The physician maintained that the search of his office by hospital officials violated the Fourth Amendment's prohibition against unreasonable searches. The Court, in a 5-4 ruling, held that searches of government offices by government employers are subject to Fourth Amendment constraints.

The Court first held that the physician had a reasonable expectation of privacy in his office, including his desk and file cabinets. The Court then considered the standard for judging whether a search of the physician's office was reasonable, holding that "the invasion of the employee's legitimate expectations of privacy" must be balanced against "the government's need for supervision, control, and the efficient operation of the workplace."[5] The Court held that the reasonableness of a search had to be determined on a case-by-case basis. In the *O'Connor* case, the Court declined to rule on whether the search of the physician's office had been reasonable because there were unresolved issues of fact for the lower court to consider.

O'Connor thus established that if a public employee has a reasonable expectation of privacy in the area or the things to be searched, a search by an employer is constitutional only if the interests of the employer in maintaining a safe and efficient workplace override the privacy interests of the employee. (This standard is less onerous than that applied to searches by law enforcement officers, discussed in the article on page 13.) *O'Connor* left to the lower courts the task of striking the appropriate balance in each case by assessing the reasonableness of the employee's expectation of privacy and the reasonableness of the employer's search in light of the employee's privacy interest. The courts' application of this standard in different situations is reviewed in the following sections.

Lower Court Rulings

There have been surprisingly few cases in which the lower courts have applied the *O'Connor* standard, but there have been a sufficient number for a pattern to emerge.

In *Showengerdt v. General Dynamics Corporation*, the court reviewed the dismissal of a federal employee for possession of pornographic materials at the workplace.[6] The materials in question were kept in the employee's locked desk in his locked office but were seized by his supervisor and a security officer. The court found that the employee had a reasonable expectation of privacy in his locked desk and office —the first inquiry required under *O'Connor*—but remanded the case for a determination of whether the government's purpose in investigating work-related misconduct outweighed the employee's Fourth Amendment privacy interest—the second *O'Connor* inquiry.

In a similar case, *Gossmeyer v. McDonald*, a child protective investigator's rights were held not to have been violated when her employer, with the assistance of law enforcement officials, conducted a warrantless search of her desk, file cabinet, and storage unit based on a co-worker's tip that she had pornographic pictures of children in her office.[7] Assessing the second *O'Connor* requirement, the court held that the search was reasonable. It found that the search was based on a tip by a co-worker, which was sufficiently reliable in that it specifically alleged where the pictures would be found; and that the search was reasonable in scope in that it was limited to places where the pictures were stored.

In *Diaz Camacho v. Lopez Rivera*, the court considered a claim by a dismissed fire chief that his Fourth Amendment rights had been violated when his employer had conducted a search of his office.[8] The court upheld the search and sustained the employee's dismissal, finding that the town officials had reasonable grounds to suspect that the fire chief was guilty of work-related misconduct and that a search of his office might turn up evidence of such misconduct. In so ruling, the court noted that the chief's office also was used to store the fire station's official records and maintenance equipment, thus creating a lower expectation of privacy than might otherwise have been the case and affecting the balance to be struck in weighing the employer's interests against the employee's.

In *Williams v. Philadelphia Housing Authority*, a supervisor's removal of her subordinate employee's computer disk from his desk was upheld.[9] The employee was on a leave of absence and had been asked to clear his desk. Because the supervisor initiated the search to look for work-related material, the court found her search to be reasonable. By contrast, in *Rossi v. Town of Pelham*, the court held that a town police officer's search of the town clerk's office for certain municipal records was unreasonable.[10] The court held that the clerk enjoyed an expectation of privacy in her office because she had exclusive access to and use of the area and the town had not placed her on notice that the office was subject to intrusions by other town officials.

In *Johnson v. City of Menlo Park*, a municipal employee was fired after a co-worker complained that he had sexually harassed her.[11] Eventually, an arbitrator ordered the employee reinstated and awarded back pay. The employee also sued the city, claiming that his Fourth Amendment rights were violated when his employer searched his desk in investigating the sexual harassment charge. The city had a written policy stating that the city reserved the right to open, inspect, and examine all equipment and workspaces at any time for legitimate business reasons, including investigating work-related misconduct. The court held that because the policy was known to the employee and made it clear that the city had the right to search the workplace, the employee did not have a reasonable

expectation of privacy in his desk. The court therefore granted summary judgment for the employer.

In *United States v. Chandler*, in which a municipal police officer left his duty bag in his locker after he was suspended, the court found that he had no reasonable expectation of privacy.[12] The internal affairs division retrieved the bag and conducted a warrantless search that yielded crack cocaine and heroin. The court held that the search did not violate the employee's Fourth Amendment rights because the bag was abandoned property. Thus any expectation of privacy was forfeited.

The court held that because the policy was known to the employee and made it clear that the city had the right to search the workplace, the employee did not have a reasonable expectation of privacy in his desk.

In *United States v. Simons*, the court considered a computer case in which the plaintiff worked for the Central Intelligence Agency (CIA).[13] He had his own computer in his office, which he did not share with anyone. The CIA had a policy authorizing electronic audits to ensure that unlawful material was not downloaded onto government computers. The policy explained, in detail, how the auditing program worked. The program included looking at sent and received e-mails, Web-site visits, and the like. The policy also stated that the agency would periodically audit, inspect, and monitor the employee's Internet access.

One of the employer's computer programmers entered the word "sex" in a search and found that the plaintiff had a large number of hits. From his own computer, the programmer examined the hard drive of the employee's computer and found more than 1,000 pornographic images, some of minors. Subsequently a manager physically entered the employee's office and removed the hard drive. Later searches, with warrants, were conducted, and other evidence was found. The Fourth Circuit Court of Appeals held that the remote searches of the employee's computer did not violate his Fourth Amendment rights because, in light of the policy, he lacked a legitimate expectation of privacy in the files downloaded from the Internet. For the same reasons, the employee's Fourth Amendment rights were not violated by the retrieval of his hard drive from his office. In addressing the actual entry into the employee's office, the court held that the employee did have a reasonable expectation of privacy, but the entry was lawful because the CIA had reasonable grounds for suspecting that the entry would yield evidence of misconduct.

Finally, in *Leventhal v. Knapek*, the court heard a claim by an accountant in a state department of transportation.[14] His supervisors received an anonymous letter that did not name him but gave his pay grade, gender, and job title. He was the only one at his pay grade in his office. The letter accused him of being late, being gone from the office half the time, doing primarily nonoffice work when he was there, and always talking to co-workers about personal computers. As a result of the letter, the supervisors conducted a computer review without his knowledge and found tax preparation programs that the employee was using for his private tax business. The employee was suspended without pay for thirty days but then challenged the right of the employer to search his computer.

The Second Circuit Court of Appeals ruled that the search did not violate the employee's Fourth Amendment rights. The employee had a reasonable expectation of privacy in the contents of his computer, the court held, but the search was reasonably related to the department's investigation into allegations of the employee's workplace misconduct.

Lessons Learned

One lesson that emerges from these cases is that it may be difficult for a public employee to assert an overriding privacy interest if his or her employer has developed and posted a policy informing employees that the workplace is subject to periodic searches.

A second lesson, though, is that even if the employee can assert a reasonable expectation of privacy, the public employer can meet the burden of showing the reasonableness of the search on the basis of a combination of factors—for example, (1) a tip by a credible coworker of misconduct (*Gossmeyer* and *Leventhal*); (2) the limited scope of the search (*Gossmeyer*); (3) a lowered expectation of privacy because of accessibility (*Diaz Camacho*); and (4) the limited purpose of the search (*Williams*).

The final lesson of these cases is that before conducting a workplace search of employees' lockers, offices, files, or other areas in which employees may fairly be said to have a legitimate expectation of privacy, employers should consider whether the need for supervision, control, and efficient operation of the facility outweighs the employees' privacy interest.

Notes

1. 17 Individual Employment Rights Reporter (Washington, D.C.: BNA Publications), May 1, 2001, at 33.
2. Katz v. United States, 389 U.S. 347 (1967).
3. *Id.* at 361.
4. O'Connor v. Ortega, 480 U.S. 709 (1987).
5. *Id.* at 719–20.
6. Showengerdt v. General Dynamics Corp., 823 F.2d 1328 (9th Cir. 1987).
7. Gossmeyer v. McDonald, 128 F.3d 481 (7th Cir. 1997).
8. Diaz Camacho v. Lopez Rivera, 699 F. Supp. 1020 (D.P.R. 1988).
9. Williams v. Philadelphia Hous. Auth., 826 F. Supp. 952 (E.D. Penn. 1993).
10. Rossi v. Town of Pelham, 13 Individual Employment Rights Cases (BNA) 1021 (D.N.H. 1997).
11. Johnson v. City of Menlo Park, 1999 WL 551241 (N.D. Cal. 1999).
12. United States v. Chandler, 197 F.3d 1198 (8th Cir. 1999).
13. United States v. Simons, 206 F.3d 392 (4th Cir. 2000).
14. Leventhal v. Knapek, 266 F.3d 64 (2nd Cir. 2001).

Privacy and Public School Students

Laurie L. Mesibov

Since September 11, 2001, many public institutions have been trying to strike the proper balance between security and privacy. In public schools, striking that balance has been the subject of intense debate, extensive policy making, and lawsuits for years. Public school students, and adults, have the same concerns about privacy. They want control over who searches their possessions and their bodies and who has access to information about them.

Students and their parents who think school officials have acted in a way that does not properly respect students' privacy may challenge the action. Occasionally the challenge results in litigation. The U.S. Supreme Court hears only a small fraction of the cases it is asked to review, so its decision to hear three cases involving student privacy in its 2001–2 term is noteworthy. This article provides a brief overview of the two issues before the Court: searches of students and student records.[1]

Searches of Students

As concerns about discipline, drugs, and violence at schools have increased, so have school officials' need and desire for authority to search students and their belongings. At the same time, schools must respect students' rights, including their right to privacy.

Everyone wants safe and orderly schools.[2] Schools are special places, with a special mission,[3] and students, in part because of their youth, need protection. The Constitution guarantees students constitutional rights, even though schools might be safer and more orderly if it did not.[4] However, when students are at school or are involved in school activities, their rights often are more limited than if they were elsewhere.[5] This certainly is true when the issue is a student's right under the Fourth Amendment to the U.S. Constitution to be free from unreasonable searches of his or her person or property.

In 1985, in *New Jersey v. T.L.O.*, the U.S. Supreme Court for the first time stated directly that the Fourth Amendment applies to schools and that students' legitimate expectations of privacy must be balanced against schools' need to maintain a safe environment for teaching and learning.[6] In that case the Court established the standard for searches of students by school officials:

- The Fourth Amendment's prohibition of "unreasonable searches" applies to searches of public school students conducted by school officials. The legality of a search of a student depends on the reasonableness, under all the circumstances, of the search.
- School officials do not need a search warrant to search a student under their control.
- School officials need "reasonable suspicion" to search a student. Reasonable suspicion is a less demanding standard than probable cause (the standard generally applied in assessing the lawfulness of a search as part of a criminal investigation).[7]
- Students have a reasonable expectation of privacy in personal articles carried inside their purses, wallets, and book bags, as well as in their clothing and on their bodies.[8]
- If a student gives a valid consent to a search, schools officials may proceed with or without reasonable suspicion. However, a student's consent may be subject to claims that the student did not understand what he or she was consenting to or that the consent was not voluntary.
- In situations in which a student has no legitimate expectation of privacy, the Fourth Amendment does not restrict searches by school officials.

As concerns about discipline, drugs, and violence at schools have increased, so have school officials' need and desire for authority to search students and their belongings.

Elements of a Reasonable Search

T.L.O. set out a two-part test to determine whether a search by school officials is reasonable under the Fourth Amendment. The first part of the test requires that a search be reasonable at its inception. This condition is met if school officials have reasonable suspicion that the search will uncover evidence that the student has violated or is violating either a law or a school rule. Reasonable suspicion may be based on personal observation or information

The author is an Institute of Government faculty member who specializes in public school law. Contact her at mesibov@iogmail.iog.unc.edu.

from others. Courts evaluating whether reasonable suspicion existed at the time of the search have considered the reliability of the information and of its source; the need to conduct an immediate search without additional information; the nature of the violation of a law or a school rule; and information that the school already had about the problem and the individual student.

The U.S. Supreme Court will soon rule on whether a school may conduct random, suspicionless drug testing of students in marching bands and other extracurricular activities.

In reaching their conclusion about the presence of reasonable suspicion, school officials are entitled to rely on "common-sense conclusions about human behavior."[9] The results of the search do not affect its reasonableness at inception. That is, positive results do not turn an unreasonable search into a reasonable one.

The second part of the *T.L.O.* test requires that the scope of the search be reasonably related to the circumstances that justified it. This means that a search must be reasonably related to its objectives and not excessively intrusive in light of the age and the sex of the student and the nature of the infraction. This requirement is the basis for many rulings finding strip searches for missing property unconstitutional.[10] Strip searches for illegal drugs, however, have more often been upheld when grounds to search have existed.[11]

Application of the *T.L.O.* Standard in North Carolina

The North Carolina Court of Appeals has decided two student search cases.[12] Neither case breaks new legal ground. In each case a student raised the issue of the involvement of "school resource officers" (law enforcement officers working regularly in public schools) in the search—a fact not present in *T.L.O.* However, the court did not find it necessary to decide whether resource officers act as law enforcement officers subject to the warrant and probable-cause requirements of the Fourth Amendment or act as school officials subject to the less demanding reasonable-suspicion standard established in *T.L.O.*

In the first case, an assistant principal found a pellet gun in a student's book bag, and, as a result, the student was adjudicated delinquent for possessing a weapon on school property.[13] The student wanted the evidence suppressed and challenged the constitutionality of the search because of the school resource officer's actions, which included handcuffing him. The court found that the assistant principal, acting on an unsolicited tip followed by the student's

The *Earls* Case: Drug Testing of Participants in Extracurricular Activities

In *Earls v. Board of Education of Tecumseh Public School District No. 92 of Pottawatomie County*, a school district policy made high school students' participation in any extracurricular activities contingent on their consenting to random, suspicionless drug testing. All students choosing to participate were required to take an initial drug test and to agree to periodic random, suspicionless testing (as well as testing if the school had individualized suspicion). Several students sued the district over the policy's application to members of the show choir, the marching band, and the academic team. (The drug testing of athletes was not challenged.)

The federal district court ruled in favor of the school board, but the Tenth Circuit Court of Appeals reversed the decision, finding that the board did not have sufficient justification for the policy. The court applied the factors that the Supreme Court used in *Vernonia*: the students' expectation of privacy, the character of the intrusion, the nature and the immediacy of the governmental concern, and the efficacy of the solution. Looking at the first two factors, the court found that participants in extracurricular activities have a somewhat lesser expectation of privacy than nonparticipants and that the invasion of privacy was not significant, given the manner in which the drug tests were conducted.

However, looking at the third factor, the court found in favor of the students. Given the paucity of evidence of an actual drug abuse problem, the immediacy of the district's concern was greatly diminished, as was the efficacy of the district's solution. The court saw "little efficacy in a drug testing policy which tests students among whom there is no measurable drug problem." The court explained that "any district seeking to impose a random suspicionless drug-testing policy as a condition of participation in a school activity must demonstrate that there is some identifiable drug abuse problem among a sufficient number of those subject to the testing, such that testing will actually redress the problem."[1]

The school board stopped the testing and appealed to the Supreme Court. The Court agreed to hear the case during its 2001–2 term.

Note

1. Earls v. Board of Educ. of Tecumseh Public Sch. Dist. No. 92 of Pottawatomie County, 242 F.3d 1264, 1277, 1278 (10th Cir.), *cert. granted*, 122 S. Ct. 509 (Nov. 8, 2001).

uncooperative and disruptive behavior when approached, had reasonable cause to search his book bag. While the search was in progress, the assistant principal asked the resource officer to help control the student. The court found that the officer was involved solely to allow the assistant principal to search the book bag without interference or danger. The *T.L.O.* standard was satisfied because a school official conducted the search and had reasonable grounds to do so.

In the second case, after a student was found in possession of a knife on public school grounds, she was adjudicated delinquent and placed on supervised probation.[14] She appealed, claiming that the knife was obtained through an unreasonable search. The principal had received information from a substitute teacher that students from another school were planning to come onto the campus to fight and that a student at the school would be involved. On the basis of his experience, the principal was concerned that the intruding students would have weapons. He, the school resource officer, and two off-duty law enforcement officers confronted the four students, all girls. The girls responded to the principal evasively and with profanity and gave false names. Shortly after their behavior and responses to his questions heightened the principal's suspicions, the resource officer searched D.D.'s purse.

The student argued that the *T.L.O.* standard should not apply because she was not enrolled in that school and because law enforcement officers participated in the investigation and the search. The court concluded that, despite the student's not being enrolled in the school, the *T.L.O.* standard was appropriate. The law enforcement officers' involvement was minimal relative to the principal's. At most they acted "in conjunction with" the principal to further his obligations to maintain a safe, educational environment and to report truants from other schools.

Searches without Individualized Suspicion

T.L.O. and many lower court cases have answered many questions regarding whether school officials have had reasonable suspicion that a search of a particular student or a specific, identifiable group of students would turn up evidence of a violation of a law or a school rule. However, one of the major questions *T.L.O.* left unresolved is the reasonableness of searches when school officials believe that a law or a school rule is being violated but do not have reasonable suspicion about a particular student or group of students. Suppose, for example, that school officials have reliable evidence that drug use among students, especially athletes, is increasingly a problem. These school officials have a legitimate concern, but they do not have "individualized suspicion" about specific students.

In settings other than schools, the U.S. Supreme Court has held that a search may be conducted without individualized suspicion when "the privacy interests implicated by the search are minimal, and . . . an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion."[15] In *T.L.O.* itself the Court indicated that exceptions to the need for individualized suspicion could be made when

> *the privacy interests implicated by a search are minimal and where "other safeguards" are available "to assure that the individual's*

Many schools have policies that permit school officials to search student lockers at any time, with or without reasonable suspicion. Such policies are assumed to eliminate any expectation of privacy in a locker. No North Carolina court has ruled on the constitutionality of this type of policy.

reasonable expectation of privacy is not 'subject to the discretion of the official in the field.'"[16]

In *Vernonia School District 47J v. Acton*, the only student search case decided by the Court since *T.L.O.*, the Court addressed the issue of mandatory random drug-testing of students participating in athletics.[17] In reaction to an increase in drug use by high school students, especially among athletes, a school district in Oregon established a mandatory urinalysis drug-testing program. Students had to consent to the tests as a prerequisite to participating in high school athletics. A student who wanted to play football refused to consent and then sued the school district, claiming that the mandatory search violated the Fourth Amendment.

The Court ruled that the search was reasonable and therefore constitutional. Reasonableness is determined by balancing the intrusion into the individual's privacy interest against the search's promotion of a legitimate government interest. The Court considered three factors: (1) the nature of the privacy interest, (2) the character of the intrusion, and (3) the nature and the immediacy of the government interest, and the efficacy of the search as a means of meeting that interest. The Court ruled that deterring drug use among athletes justified the policy, in light of the district's evidence that a problem existed, the athletes' lowered expectation of privacy inherent in participation in sports, and the minimal intrusion on student privacy because of the manner in which the drug tests were conducted.

The Court did not rule on the issue of random, suspicionless drug testing of all students or even of students participating in extracurricular activities besides athletics.[18] Challenges to school policies involving suspicionless testing since *Vernonia* have had mixed results; courts have decided in favor of students in some cases and in favor of school officials in others.[19]

A clearer picture of the constitutionality of these searches should soon emerge. The U.S. Supreme Court has agreed to hear *Earls v. Board of Education of Tecumseh Public School District No. 92 of Pottawatomie County*,[20] and its decision will clarify the scope of *Vernonia*. (For the details of the *Earls* case, see the sidebar, opposite.)

Student Records

A second issue involving student privacy arises inevitably in schools. Schools gather and maintain a wealth of information about the students whom they enroll: academic performance, health, race, family, disciplinary actions, attendance, extracurricular activities, socioeconomic status, and involvement with the department of social services and law enforcement agencies.

Not surprisingly, school officials frequently find themselves balancing the need to disclose information about an individual student against the student's interest in keeping the information confidential. In this balancing, school officials' choices are guided by the federal Family Educational Rights and Privacy Act of 1974, commonly known as FERPA or the Buckley Amendment.[21] FERPA applies to all public schools in North Carolina and to the State Department of Public Instruction because these entities receive federal funds.

FERPA resolves many issues related to confidentiality of student records. This statute was enacted nearly thirty years ago for two purposes.[22] First, FERPA ensures that parents, those acting as parents, and students once

they turn eighteen have access to the information that a school or a state education agency maintains about a student.[23] Second, FERPA protects students' privacy by prohibiting disclosure of information about them without parental consent except in situations in which Congress has decided that the benefits of disclosure outweigh the benefits of confidentiality. Sometimes the need to share information is obvious, as in a medical emergency or when a child enrolls in a new school. At other times, such as for certain educational research projects, the benefit is less direct but nonetheless real.

FERPA does not control access to all information that school employees have about students. It controls access only to "education records," those records that are directly related to a student and maintained by an education agency or institution or by a person acting for the agency or the institution.[24] It makes no difference whether the information is located in the student's official record, in the special education office, or in the central office.

By contrast, observations that a school employee makes about a student but does not record are not education records. Also, records that instructional, supervisory, and administrative personnel make and keep for themselves as memory aids (known as "sole possession notes") are not education records if they are not available to anyone other than a temporary substitute for the record maker.[25]

FERPA establishes several basic rights for parents:

- Parents have the right to be informed about their rights under FERPA.
- Parents may inspect and review their child's education records but only records with information about their child.
- Parents may request that a school change the information in their child's records if they believe that the information is inaccurate or misleading or otherwise in violation of the child's privacy rights. Parents have the right to a hearing to challenge the contents of the education records. They also have the right to place their own statement in the child's records explaining their view about the contested information. This statement must accompany the contested information if it is disclosed to anyone.
- Parents have the right to control the disclosure of the information in their child's education records unless a specific exception allows the school to disclose information without the parent's consent.

FERPA Cases before the U.S. Supreme Court

The *Gonzaga University* Case: Individual Lawsuits for Damages

A former student, John Doe, sued Gonzaga University (Spokane, Washington) for violating his rights under FERPA, along with other claims. Doe argued that Gonzaga had disclosed confidential information about him, without his consent, to the Office of the Superintendent of Public Instruction, the Washington state agency that certifies teachers. Doe charged that university officials had ruined his chances for a teaching career by telling the agency that he allegedly had raped another student. A jury agreed and awarded Doe $150,000 in damages for the FERPA violation, along with damages for other claims. The state court of appeals reversed the jury award.[1] Doe appealed to the state supreme court.

One issue facing the court was whether individuals can sue for damages for FERPA violations. Several courts have held that FERPA itself does not give rise to a private cause of action.[2] However, Doe used the FERPA violation as the basis for a claim under a federal civil rights statute that provides a remedy for federally conferred rights. The act is popularly known as Section 1983 for its location in the United States Code.[3] The state supreme court ruled that FERPA does give rise to a federal right enforceable under Section 1983.[4] The U.S. Supreme Court has agreed to review this decision.[5]

The *Falvo* Case: The Meaning of "Education Records"

On November 27, 2001, the U.S. Supreme Court heard a case, *Owasso Independent School District v. Falvo*, dealing with a FERPA issue so basic that its not having been resolved long ago is surprising. The issue is the meaning of the term "education records." Specifically the issue is whether, in the absence of parental consent, allowing students to grade one another's homework and tests as their teacher goes over the correct answers aloud in class violates FERPA's prohibition against the release of education records.

Kristja Falvo's children attended public school in Oklahoma. Some of their teachers had them exchange papers and grade one another's work. When students got their own papers back, they called out their grades to the teacher. Falvo complained to the school counselors and the superintendent that this practice embarrassed her children. Although the school offered the children the option of confidentially reporting their grades to the teacher, the school district was not willing to issue a flat ban on students' trading papers. Falvo sued the district, claiming that the practice violated both the privacy rights implicit in the Fourteenth Amendment and FERPA.

The district court found no violation of either the Fourth Amendment or FERPA. Falvo appealed. The Tenth Circuit Court of Appeals found no violation of the Fourth Amendment but ruled that allowing students to grade one another's papers, even without calling out grades to the teacher, violates FERPA by allowing the disclosure of education records without parental consent.[6] (Remember that FERPA defines "education records" as records that contain information directly related to a student and that

- Parents have the right to complain to the FERPA Office in the federal Department of Education if they believe the school has violated FERPA.

Schools must respect these rights and fulfill corresponding responsibilities. First, schools must notify parents annually of their rights under FERPA. Further, schools must maintain a record showing all organizations, agencies, and individuals (except school officials and employees) that have requested or obtained access to a student's education records and indicating the legitimate interest each had in obtaining the information.

Most important, school officials must have specific written consent from a student's parent before disclosing personally identifiable information in that student's education records (or before giving access to the records themselves) unless disclosure is made under one of the exceptions in FERPA.[26] The most significant exceptions are as follows:[27]

- Disclosure to other school officials, including teachers, with a legitimate educational interest. For example, a teacher who is having problems with a student may look at the student's records to learn whether the problem is new or has been addressed previously. A teacher who is merely curious about a student's academic performance or disability status, however, has no legitimate educational interest and should not have access to the records.
- Disclosure in connection with an emergency if information is necessary to protect the health or safety of the student or other people.
- Disclosure to another school or school system in which the student seeks or intends to enroll. The student's parents must be notified of the disclosure and receive a copy of the records that were sent to the enrolling school if they want a copy.
- Disclosure in response to a judicial order or pursuant to a lawfully issued subpoena.[28] A school must make reasonable efforts to notify the parents in advance of disclosing the information.
- Disclosure to state and local officials in connection with the state's juvenile justice system, under specific conditions.
- Disclosure to organizations conducting studies for, or on behalf of, education agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, or improving instruction, with conditions.

are maintained by an education agency or institution or by a person acting for the agency or the institution.) The court explained that when one student puts a grade on another student's paper at the teacher's direction, and then the teacher records at least some of the grades for his or her use (as the teacher did), the first student is acting "for the school district." The school board appealed, arguing that student work that is created, used, or kept in the classroom and not made part of a student's institutional record does not meet the definition of education record.

The U.S. Supreme Court announced its decision in February 2002. In a 9-0 ruling, it reversed the decision of the court of appeals, holding that peer grading does not violate FERPA.[7] The Court explained that student papers in the hands of other students for grading are not education records. The papers do not meet the statutory definition because they are not records "maintained" by the school, nor are the students "acting for" the school. In addition, the Court noted that under the court of appeals' interpretation of FERPA, the federal government would become more involved in specific teaching methods and instructional dynamics in classrooms than Congress is likely to have mandated.

The holding in the case is limited to the narrow point that, assuming a teacher's grade book is an education record, grades on students' papers are not covered by FERPA before the teacher has recorded them. The Court did not decide whether grades on individual assignments are education records once the teacher has recorded them. However, it did say that FERPA "implied" that education records are institutional records kept by a single central custodian, such as a registrar. Justice Antonin Scalia, though concurring in the judgment, disagreed with that view.

Notes

1. Doe v. Gonzaga Univ., 992 P.2d 545 (Wash. App. 2000).
2. Fay v. South Colonie Cent. Sch. Dist., 802 F.2d 21 (2d Cir. 1986), Tarka v. Cunningham, 917 F.2d 890 (5th Cir. 1990).
3. 42 U.S.C. § 1983.
4. Doe v. Gonzaga Univ., 24 P.3d 390 (Wash. 2001), *cert. granted*, 122 S. Ct. 865 (2002). The Washington Supreme Court relied on Blessing v. Freestone, 520 U.S. 329, 329–30 (1997). The Court in that case held that, to determine whether a particular statutory provision gives rise to a federal right, a court must examine three factors: (1) whether Congress intended the provision in question to benefit the plaintiff, (2) whether the right protected by the statute is so vague and amorphous that its enforcement would strain judicial competence, and (3) whether the statute imposes a binding obligation on the states.
5. In the *Falvo* case, discussed in the next section of this sidebar, the U.S. Supreme Court assumed, without deciding, that FERPA provides private parties with a cause of action enforceable under Section 1983.
6. Falvo v. Owasso Indep. Sch. Dist. No. I-011, 233 F.3d 1203 (10th Cir. 2000), *rev'd*, 534 U.S. ___ (Feb. 19, 2002), available at www.supremecourtus.gov/opinions/01/pdf/00-1073.pdf (visited Feb. 25, 2002).
7. Owasso Indep. Sch. Dist. No. I-011 v. Falvo, 534 U.S. ___ (Feb. 19, 2002, available at www.supremecourtus.gov/opinions/01/pdf/00-1073.pdf (visited Feb. 25, 2002).

- Disclosure to accrediting organizations to carry out their accrediting functions.
- Disclosure of directory information, if certain conditions are met. "Directory information" is information in education records that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the student's name, address, telephone number, date of birth, awards, and participation in officially recognized activities.[29] Directory information may be disclosed without consent only if parents have been told that such disclosure is possible and have been given the opportunity to direct the school not to disclose any directory information about their child.

If a school official violates FERPA, the U.S. Department of Education may investigate and then may terminate federal financial assistance, but only if the secretary of education finds that the school has failed to comply and will not comply voluntarily. This simply does not happen: schools that have not complied with the law promise to comply in the future. Although cutting off federal aid is the sole remedy in FERPA itself, in a few cases, parents have successfully sued for damages under another federal statute.[30] The U.S. Supreme Court has agreed to review a case that presents this issue (see the sidebar on page 40).

FERPA's fundamental principles are clear and can be outlined even in this very brief summary. Although these principles are well understood and the statute and its regulations[31] specifically address many situations faced by school officials, new questions about FERPA's meaning continue to be litigated. In addition to the question of whether parents may sue for violations of FERPA, the U.S. Supreme Court recently decided a case involving the definition of "education records" (see the sidebar on page 40).

Conclusion

This article only skims the surface of two student privacy issues: searches at school and education records. Even within these two areas, many issues have not been fully discussed—for example, the confidentiality of special education records, searches of students' lockers, and use of metal detectors and drug-detection dogs. Other privacy issues have not been addressed at all, among them the confidentiality of information told to a school counselor, limitations on gathering certain personal information, disclosure of information to and from the juvenile justice system, and the use of students as research subjects.[32]

Nonetheless, several conclusions may be drawn from this discussion. First, the days when school officials were considered as acting in place and on behalf of parents are gone, at least within this context. Second, students have privacy interests that must be respected by school officials. Third, these officials have substantial guidance from the well-developed law of student searches and student records. Fourth, important questions about searches and records remain unresolved, though some of them will be answered this year. Finally, the law affecting student privacy will continue to evolve as school officials and students operate in a changing school environment.[33]

Notes

1. For a more comprehensive review, *see* EDUCATION LAW IN NORTH CAROLINA (Janine M. Murphy ed.; Chapel Hill: Principals' Executive Program, The Univ. of N.C. at Chapel Hill, 2001); and JAMES RAPP, EDUCATION LAW (Newark, N.J.: Matthew Bender, 2001).

2. "The General Assembly finds that all schools should be safe, secure, and orderly. If students are to aim for academic excellence, it is imperative that there is a climate of respect in every school and that every school is free of disruption, drugs, violence, and weapons. All schools must have plans, policies, and procedures for dealing with disorderly and disruptive behavior." N.C. GEN. STAT. § 115C-105.45 (hereinafter G.S.). "Each local board of education shall develop a local school administrative unit safe school plan designed to provide that every school in the local school administrative unit is safe, secure, and orderly, that there is a climate of respect in every school, and that appropriate personal conduct is a priority for all students and all public school personnel." G.S. 115C-105.47(a).

3. "It is the intent of the General Assembly that the mission of the public school community is to challenge with high expectations each child to learn, to achieve, and to fulfill his or her potential." G.S. 115C-105.20. "It is the policy of the State of North Carolina to create a public school system that graduates good citizens with the skills demanded in the marketplace, and the skills necessary to cope with contemporary society. . . ." G.S. 115C-408.

4. Tinker v. Des Moines Indep. Sch. Dist., 393 U.S. 503, 511 (1969).

5. Students' rights often are more limited than those of adults. School officials' power over students is "custodial and tutelary, permitting a degree of supervision and control that could not be exercised over free adults." Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 655 (1995).

6. New Jersey v. T.L.O., 469 U.S. 325 (1985).

7. For a discussion of the reasonable-suspicion standard as it applies in criminal cases, see the article on page 13.

8. For a discussion of the meaning of "reasonable expectation of privacy" in the context of criminal and employment matters, see the articles on pages 13 and 33.

9. *In re* Murray, 136 N.C. App. 648, 652, 525 S.E.2d 496, 499 (2000), quoting United States v. Cortez, 449 U.S. 411, 418 (1981).

10. Thomas v. Roberts, 261 F.3d 1160 (11th Cir. 2001) (holding that strip searches of fifth graders for missing $26 were unconstitutional).

11. Williams v. Ellington, 936 F.2d 881 (6th Cir. 1991), Cornfield v. Consolidated High Sch. Dist. 230, 991 F.2d 1316 (7th Cir. 1993) (approving strip searches because illegal drugs can be concealed on person's body).

12. A state court might find that its state constitution requires adoption of a standard for searches of students that is stricter than the *T.L.O.* standard. The N.C. Court of Appeals did not do this; it adopted the *T.L.O.* standard.

13. In re *Murray*, 136 N.C. App. 648, 525 S.E.2d 496.

14. *In re* D.D., ___ N.C. App. ___, 554 S.E.2d 346 (2001), *review denied*, 2001 N.C. LEXIS 1294 (N.C. Dec. 18, 2001).

15. Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624 (1989).

16. New Jersey v. T.L.O., 469 U.S. 325, 342 n.8 (1985), quoting Delaware v. Prouse, 440 U.S. 648, 654–55 (1979).

17. Vernonia School District 47J v. Acton, 515 U.S. 646 (1995).

18. "I comprehend the Court's opinion as reserving the question whether the District, on no more than the showing made here, constitutionally could impose routine drug testing not only on those seeking to engage with others in team sports, but on all students required to attend school." *Id.* at 666 (Ginsburg, J., concurring).

19. Willis v. Anderson Community Sch. Dist., 158 F.3d 415 (7th Cir. 1999) (striking

School officials may search a student's book bag if they have reasonable suspicion that the bag contains evidence of a violation of a law or a school rule.

down policy that required all suspended students to submit to drug test at end of suspension, because there was no causal connection between offense of fighting and suspicion of drug use); Todd v. Rush County Sch., 133 F.3d 984 (1998) (upholding on health and safety rationale, random drug testing of all students who wanted to participate in extracurricular activities or park at school); Joy v. Penn-Harris-Madison Sch. Corp., 212 F.3d 1052 (7th Cir. 2000) (upholding drug and alcohol testing of students participating in extracurricular activities or parking at school, because court was bound by precedent of *Todd v. Rush;* striking down policy requiring testing student drivers for nicotine); B.C. by and through Powers v. Plumas Unified Sch. Dist., 192 F.3d 1260 (9th Cir. 1999) (striking down random, suspicionless search of students by drug-sniffing dogs, in absence of evidence of drug problem); Tannahill *ex rel.* Tannahill v. Lockney Indep. Sch. Dist., 133 F. Supp. 2d 919 (N.D. Tex. 2001) (striking down policy requiring consent to random drug tests as condition of participation in extracurricular activities, because testing program was not specifically targeted to special needs of drug crisis).

20. Earls v. Board of Educ. of Tecumseh Public Sch. Dist. No. 92 of Pottawatomie County, 242 F.3d 1264 (10th Cir.), *cert. granted*, 122 S. Ct. 509 (Nov. 8, 2001).

21. 20 U.S.C. § 1232g. FERPA is the most important statute controlling access to student records. Other federal statutes and some state statutes also affect the privacy of student records. For a more detailed discussion, *see* Thomasin Hughes, *Releasing Student Information: What's Public and What's Not*, 32 SCHOOL LAW BULLETIN 12 (2001).

22. Traditional legislative history of FERPA as first enacted in 1974 is not available because it was offered as an amendment sponsored by Senator James Buckley rather than being the subject of committee consideration. The Joint Statement in Explanation of Buckley/Pell Amendment, the major source of legislative history for the amendment, was introduced several months later. It is available at www.ed.gov/offices/OM/fpco/Legislativehistory.html (visited Feb. 7, 2002).

23. This article uses "parent" to cover all adults who have decision-making authority under FERPA (an eligible student, a parent, a guardian, a custodian, or a person acting in place of a parent). "Eligible student" means a student who has reached eighteen years of age or is attending an institution of postsecondary education. "Parent" means a parent of a student and includes a natural parent, a guardian, or an individual acting as a parent in the absence of a parent or a guardian. 34 C.F.R. § 99.3.

24. 20 U.S.C. § 1232g(a)(4). A "record" is any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audiotape, film, microfilm, and microfiche. 34 C.F.R. § 99.3.

25. 20 U.S.C. § 1232g(a)(4); 34 C.F.R. § 99.3.

26. 20 U.S.C. § 1232g(a)(4). Note that when FERPA allows a school board to disclose information, it does not mandate that the board do so. Other statutes and policies may require the board to disclose information when FERPA allows it.

27. 34 CFR § 99.31.

28. John Rubin, *Subpoenas and School Records: A School Employee's Guide*, 30 SCHOOL LAW BULLETIN 1 (1999).

29. 20 U.S.C. § 1232g(a)(4).

30. Fay v. South Colonie Cent. Sch. Dist., 802 F.2d 21 (2d Cir. 1986), Tarka v. Cunningham, 917 F.2d 890 (5th Cir. 1990) (both holding that parent or student may bring FERPA claim under 42 U.S.C. § 1983, which allows lawsuits when claim is that right protected by federal statutes has been violated).

31. 34 C.F.R. § 99.

32. For information on limitations on gathering certain personal information, *see* the Hatch Amendment, codified at 20 U.S.C. § 1232h. For information on disclosure of information to and from the juvenile justice system, *see* www.ed.gov/offices/OESE/SDFS/actguid/infshare.html (visited Feb. 7, 2002).

33. For additional information, readers may consult their local school boards, use the resources cited in note 1, and research privacy issues online. Two useful sites are www.ed.gov (the federal Department of Education) and www.dpi.state.nc.us (the State Department of Public Instruction and the State Board of Education).

Health Privacy: The New Federal Framework

Aimee N. Wall

Patients usually expect that health information shared and generated when they are receiving medical care will be kept confidential by their health care provider and, if they have insurance, by their health insurance plan. A recent Gallup survey found that almost 78 percent of adults believe it is "very important" that their health information be kept confidential.[1] Most providers and insurers strive to meet these expectations. However, other people and organizations often need access to health information to carry out their responsibilities. For example, public health officials want health care providers to report communicable diseases, law enforcement officials expect emergency care providers to report gunshot wounds, and social services agencies rely on health care providers to report evidence of abuse or neglect.

For many years, federal, state, and local lawmakers have struggled to find the appropriate balance between protecting the privacy of health information and ensuring that health information is available when necessary for other important purposes. A patchwork of federal and state laws, rules, common law, and professional ethical obligations and guidelines has resulted, providing a hazy outline at best for when providers and insurers may share health information with other entities. This past year, however, the first and only *comprehensive* federal rule on health privacy went into effect.[2] This article provides a brief history of the new rule, summarizes many of the rule's complex requirements, and offers a few suggestions for entities and local governments, particularly counties, to consider as they begin to comply.

Why Is the New Rule Necessary?

Until recently the federal government approached the issue of privacy in a piecemeal fashion. Several laws dealt with health information privacy but did not regulate it comprehensively. For example, most information held by the federal government that identifies individuals is subject to the Privacy Act of 1974;[3] health information held by substance abuse programs receiving federal assistance is subject to a substance abuse confidentiality rule;[4] and information held by providers treating Medicare and Medicaid patients is subject to an array of confidentiality statutes and rules.[5]

Similarly every state has health privacy laws, but only a handful are comprehensive.[6] The vast majority of states, including North Carolina, have limited laws governing only particular types of entities, such as HMOs,[7] or specific conditions, such as communicable diseases.[8]

The result of this piecemeal approach has been that under most circumstances, people could not be assured that health care providers, insurers, or others were legally required to keep health information confidential.[9] Many argued that the legal framework was fractured and wholly inadequate to protect information.[10]

As health care delivery entered the electronic age, concerns about privacy increased. The health care industry began to integrate technological tools into the practice of medicine—for example, electronic medical records,

The author, an Institute of Government faculty member who specializes in public health law, frequently advises local health departments about health information privacy. Contact her at wall@iogmail.iog.unc.edu.

"telemedicine" (the use of telecommunications to support long-distance clinical care), and electronically filed insurance claims. The industry appealed to Congress for legislation to facilitate electronic sharing of information between providers and insurers. Congress passed such legislation as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). One part of this legislation, entitled Administrative Simplification, directed the U.S. Department of Health and Human Services (DHHS) to develop a series of rules that would standardize the electronic sharing of health information and dramatically reduce administrative expenses.

A doctor's laptop was stolen at a medical conference. The computer contained the names and medical histories of his patients in North Carolina.

From A. Santana, *Thieves Take More than Laptops*, WASHINGTON POST, Nov. 5, 2000, at A1

Congress recognized, however, that because Administrative Simplification would encourage health information to flow more freely, preserving the confidentiality of that information had to become a high priority at the federal level. Therefore, as part of Administrative Simplification, Congress also directed DHHS to develop rules governing both the privacy and the security of health information. Privacy and security are closely connected but distinct concepts. Privacy is "the patient's right over the use and disclosure of his or her own personal health information," whereas security is the "specific measures a health care entity must take to *protect* personal health information from unauthorized breaches of privacy."[11]

In recognition of this difference, DHHS is developing separate rules for privacy and security. The security rule was proposed in 1998 but has not yet been finalized. The privacy rule, which is the focus of this article, was finalized during the Clinton Administration, and the compliance date is currently April 14, 2003, for most health care providers and insurers.[12] In March 2002 the Bush Administration proposed several significant revisions to the privacy rule.[13] After the public has had an opportunity to comment on the proposed revisions, DHHS will consider whether to adopt any changes recommended by the public, and then it will publish another final privacy rule. DHHS has indicated that compliance with the rule is still expected by April 2003, although Congress could delay the compliance date.

What Do Local Governments Need to Do?

The privacy rule requires "covered entities"—public and private health plans, health care clearinghouses, and most health care providers (those that transmit health information electronically)—to make significant administrative and organizational changes in the way that they handle health information. Many different components of local government will be affected by this new rule either directly or indirectly. For example, local health departments, area mental health authorities, and emergency medical service agencies are directly regulated because they are health care providers. Jail health programs and social services agencies also may be regulated entities. Law enforcement officials, courts, and medical examiners may not be covered entities, but because they often need health information from covered entities, such as health departments, social services agencies, and private health care providers, the new restrictions on disclosure will affect their ability to carry out their duties.

Given that the compliance date is fast approaching, state and local governments must immediately begin making some changes. In North Carolina, efforts are well under way at the state level to bring state agencies into compliance with the privacy rule. Last October, the General Assembly directed the Office of State Budget and Management to develop a strategic plan for implementing HIPAA.[14]

By contrast, local governments are in many different stages of readiness to comply. Some counties have only a basic awareness of the new law, whereas others have developed a strategic plan, hired a privacy officer, and are working toward compliance. Local governments should be taking a careful look at their operations and developing a compliance plan.

If it has not already done so, a county should immediately appoint a compliance officer, preferably an attorney, to become familiar with the privacy rule and oversee its implementation throughout the county. Once the officer understands the rule, he or she should determine which components of local government are covered entities, such as local health departments and jail health programs (see the later

Helpful HIPAA Web Sites

U.S. Department of Health and Human Services, Office of Civil Rights
www.hhs.gov/ocr/hipaa/

North Carolina HIPAA Program Management Office
dirm.state.nc.us/hipaa/

UNC–Chapel Hill, Institute of Government and School of Public Health Medical Privacy Training
www.medicalprivacy.unc.edu

North Carolina Healthcare Information and Communications Alliance, Inc.
www.nchica.org

New Individual Rights

Arguably the most revolutionary aspect of the HIPAA privacy regulations is the establishment of several new individual rights. The basic principle underlying these new rights is that people should be able to understand how their health information is used and disclosed and have some opportunity to control it. The privacy rule establishes several rights intended to ensure that individuals are able to control their health information, including the right to a notice of privacy practices, the right to inspect and amend health information, the right to receive a disclosure history, and the right to request certain restrictions on disclosure. Covered entities, including all local health departments and area mental health authorities, will need to develop and implement policies and procedures to accommodate these new rights.

Right to Notice

The key to gaining control over one's health information is having a clear and accurate understanding of how that information is used and shared with others. As DHHS explained, "One of the goals of this rule is to create an environment of open communication and transparency with respect to the use and disclosure of . . . health information."[1] Therefore the privacy rule creates an individual right to a notice of privacy practices that covered entities must develop and disseminate to patients and enrollees.[2]

This notice is not a simple statement saying, "We will keep your personal health information confidential." Rather, the notice is intended to be a fairly comprehensive inventory of how the entity may use and disclose health information and an explanation of the individual's rights and the entity's legal duties with respect to that information. The rule outlines the types of information that must be included in the notice and requires that it be drafted in "plain language." It is extremely important that these notices be drafted carefully and updated regularly because covered entities are bound by their notices. In other words, if they use or disclose health information in a way that is not specified in their notice, they could be subject to civil or criminal penalties.

Right of Access and Amendment

In addition to understanding how health information is used and shared, a patient must have access to that information in order to know exactly what information is being used and shared. The privacy rule therefore establishes a right to inspect and obtain a copy of most health information held by covered entities. The rule sets out several circumstances in which a patient's request for access may be denied, such as when the information requested is psychotherapy notes or has been compiled for legal or administrative proceedings. A request for access also may be denied if a health care professional determines that access is "reasonably likely to endanger the life or physical safety of the individual or another person."[3] If a covered entity denies a request, in some situations an individual may request that the decision be reviewed. The entity must act on such a request within sixty days, and it may charge a reasonable, cost-based fee for a copy of the information.

Now that patients have the right of access, it is only logical that they also be provided with the right to have the covered entity amend information that patients find to be inaccurate or incomplete.[4] The entity may deny an amendment request for a variety of reasons. Most important, it may deny a request if it determines that the information is in fact accurate or complete. If the entity does deny a request, the patient has the right to submit a "statement of disagreement," which must be kept with the record and

Continued on page 47

section headed "Who Is Regulated?"). It is possible that the entire county will be considered a covered entity. In such a case, the county's compliance officer still will need to identify the components of the county that must comply with the rule.

In addition to identifying covered entities, the county should identify other components of local government that use and share health information, and evaluate whether and how those components can continue obtaining health information from covered entities after the compliance date. For example, the privacy rule places new restrictions on when law enforcement officials may obtain health information without a court order. The compliance officer must evaluate the current practices of law enforcement officials and determine if any changes need to be made in order to ensure that the officials can obtain health information when necessary.

Once a county has identified all the local entities that will be directly and indirectly affected by the rule, it should develop a countywide compliance plan. Just as the state has designated a HIPAA Program Management Office to oversee the state's implementation, counties would be prudent to consider centralizing compliance activities at the county level. In addition, a regional approach may be appropriate in the case of area mental health authorities or public health districts. Although each county component will encounter unique challenges to implementation, having a coordinated and comprehensive countywide plan for ensuring that the April 2003 deadline is met will be worthwhile. (For a list of steps that an entity should take to move toward compliance within the necessary timeframe, see the sidebar on page 48. For Web resources, see the sidebar on page 45.)

Who Is Regulated?

When Congress passed HIPAA, it specifically limited the scope of the law to three types of entities: health care providers, health plans, and health care clearinghouses (defined later).[15] Many other groups—for example, employers, courts, researchers, and marketers—regularly handle personal health

Continued from page 46

disclosed with the record any time that the entity shares the disputed information with another entity.

If the entity accepts a request for an amendment, it need not alter the actual record but must identify the affected information and either append the amendment or provide a link in some way to the amendment. After accepting the amendment, the entity is required to make reasonable efforts to notify certain other entities that received the inaccurate or incomplete information. The entity must act on an individual's request for amendment within ninety days.

Right to an Accounting of Disclosures

To keep track of where his or her health information is going, a patient now is able to request a disclosure history from a covered entity—basically an accounting of each time that the entity has disclosed identifiable health information to other entities in the previous six years.[5] The history will provide the patient with important information about disclosures made without his or her permission, such as certain disclosures to researchers or government officials.

The history does not have to include any of the standard disclosures that an entity makes for purposes of treatment, payment, or health care operations (business practices like quality assurance that require the use of health information)—most likely the vast majority of disclosures. The history also may exclude certain other types of disclosures, such as those from a hospital's patient-information line.

Right to Request Additional Protections

The privacy rule also provides individuals with two new tools to help them gain control over how their information is disclosed.[6] First, they have the right to request that health care providers and health plans make special arrangements for communicating directly with them. For example, a patient may request that her provider or health plan send all communications (bills, test results, and so forth) to a work address rather than a home address. The provider must accommodate such a request. The health plan, meanwhile, must accommodate such a request only if the patient "clearly states that the disclosure of all or part of [the] information could endanger the individual."

Second, patients have the right to request certain restrictions on the use or the disclosure of their health information. For example, a patient may request that a provider not disclose his information for research purposes. This second right is not particularly strong because it is only the right to *request*—the entity is not required to accept the request. However, if the entity does accept the request, it is bound by the request (except in emergency circumstances), so a disclosure in violation of the request would be considered a violation of the privacy rule.

Notes

1. Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,549, 82,820 (Dec. 28, 2000).
2. 45 C.F.R. § 164.520.
3. 45 C.F.R. § 164.524. Before the privacy rule, about half of the states, including North Carolina, provided some statutory rights of access. *See, e.g.*, N.C. GEN. STAT. § 58-39-45 (hereinafter G.S.) (requiring certain insurance institutions to provide individuals with access to certain information); G.S. 122C-53(c) (requiring facilities providing treatment to people who are mentally ill, developmentally disabled, or substance abusers to provide access under certain circumstances).
4. 45 C.F.R. § 164.526.
5. 45 C.F.R. § 164.528.
6. 45 C.F.R. § 164.522.

information, but they are not covered by the privacy rule because DHHS does not have the legal authority to include them. If an entity is covered, it must comply with the privacy rule and will be subject to significant criminal and civil monetary penalties for violations.[16]

The privacy rule broadly defines "health care provider" to include any "person or organization who furnishes, bills, or is paid for health care in the normal course of business."[17] The rule applies only to providers that transmit health information electronically in connection with one of several types of health care transactions (for example, health insurance claims). Once a provider conducts such a transaction, all the individually identifiable health information held by that provider is covered by the rule. Almost all providers, including *all* local health departments and area mental health authorities, conduct some form of electronic transaction, either through their own business office or through a contract with a third-party billing company. As a result, only a handful of providers are likely to be exempt from the privacy rule. For example, a small jail health program or private free clinic might not submit any insurance claims electronically and therefore would not be covered.

By contrast, all health plans and health care clearinghouses are required to comply. "Health plan" is defined to include not only traditional private health insurance plans like Aetna and Blue Cross/Blue Shield but also public insurance programs, including Medicare, Medicaid, and the State Children's Health Insurance Program (known as Health Choice in North Carolina).[18] If a county self-insures to provide employee health insurance, it will most likely be covered by the privacy rule as a health plan. A "health care clearinghouse" is, in general, an entity (public or private) that translates health information from one data format to another.[19] It is unlikely that a county operates a health care clearinghouse, although it may contract with one.

Even though the privacy rule technically covers only these three types of entities, DHHS indirectly extended the reach of the rule to some noncovered

entities by requiring covered entities to have contracts with their business associates. A "business associate" is a third party that uses identifiable health information to provide services to or for the covered entity or otherwise assist the entity with its activities—for example, a billing company, an accountant, an attorney, or a consultant.[20] The rationale for expanding the scope of the rule is that if it were restricted to the three types of entities, individuals could not be assured that their health information would be protected. In other words, once the information traveled from a covered entity to a noncovered one, the privacy rule would become meaningless because it could no longer protect the information, and in many instances, no other law would be available to protect the information.[21] For example, if a health department contracted with a vendor to file insurance claims and bill individuals for health services, the vendor would most likely not be a covered entity, and theoretically it could choose to use, disclose, or even sell a list of patients treated by the health department.[22] Under the privacy rule, the health department must enter into a contract with the vendor that requires protection of the information.

The biggest problem with this contractual requirement is that only the covered entity, not the business associate, is subject to DHHS enforcement. Therefore, DHHS can hold only the covered entity responsible if the business associate breaches the contract and discloses health information inappropriately.[23] In response to public comments, DHHS stated that the regulatory authority provided by the underlying statute, HIPAA, was too limited and admitted that such indirect regulation of business associates was not the ideal approach but was necessary to ensure that the information was protected. DHHS has therefore encouraged Congress to pass new legislation that would allow these entities to be regulated directly.[24]

What Information Is Regulated?

The rule applies to health information that identifies individuals, in any form or medium, including electronic, paper,

What Should a Covered Entity Do Now?

To comply with the new privacy rule by April 2003, covered entities should be taking action now. Suggested steps follow.

Designate a privacy officer. He or she should understand all the requirements of the privacy rule, as well as any other applicable federal and state privacy laws. The officer should be responsible for overseeing implementation of the privacy rule within the entity, providing training or organizing training for other members of the entity's workforce, and monitoring compliance.

Conduct a "gap analysis." Review current information-sharing practices in order to compile a comprehensive inventory of how health information is used within the entity and disclosed to outside people or entities. Identify business associates—that is, third parties that use identifiable health information in providing services to a covered entity. Focus on situations or relationships in which information is currently used or disclosed in a way that violates the privacy rule.

Develop a compliance plan. This plan should begin with the gap analysis, include all the steps necessary to come into compliance, and end with an ongoing plan for monitoring compliance. Entities should work with experienced attorneys or compliance officers in developing and implementing the plan.

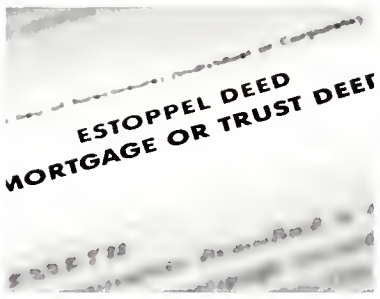
Develop and maintain privacy policies and procedures. Each entity's policies and procedures must be comprehensive, and they must be reviewed regularly to ensure that they reflect the entity's current practices as well as changes in state or federal law. Entities must maintain a written or electronic copy of their policies and procedures.

Review current forms and notices. Review current consent and authorization forms (for example, release of information, or ROI, forms) and any notices that are provided to patients. Consult with an attorney to prepare new forms and a notice of privacy practices that are consistent with the privacy rule. As with the entity's policies and procedures, these forms and notices must be kept up-to-date and accurate.

Develop training. The rule requires each entity to train its workforce on its policies and procedures before the compliance date (April 2003); to train new employees within a reasonable period after they join the workforce; and periodically to retrain any employee affected by a material change in law, policy, or procedure. The training should not only outline the requirements of the rule but also reflect all applicable federal and state laws and the agency's *own* policies and procedures.

Consider developing a coalition. Hundreds of entities throughout the state will be working at the same time on compliance. Although each entity will have to address particular needs and practices, creating a coalition of similar entities (such as local health departments in a region) that can work together toward compliance may be worthwhile. For example, the coalition might serve as an advisory group, develop a core set of policies and procedures, prepare draft forms and notices, and offer common training to the workforces of coalition members.

and even oral information. Critics of the rule argued that it is far too expansive and that Congress intended DHHS to regulate only electronically transmitted information. In reponse, DHHS asserted that Congress authorized the regulation of all health information and that this approach was the most reasonable and practical means available. Specifically, DHHS explained that limiting the application of the rule to electronically transmitted information would have created an "artificial boundary" because information is constantly moving from one format to another.[25] For example, a health care provider may submit a claim to Medicaid electronically, print out a copy of the claim, and discuss it with a co-worker. In this example, only the format of the information, not the content, has changed. The privacy rule would not adequately protect the *content* of the information if the rule was limited to electronically transmitted information.[26]



A banker who also served on his county's health board cross-referenced customer accounts with patient information. He called due the mortgages of anyone suffering from cancer.

From M. Lavelle, *Health Plan Debate Turning to Privacy: Some Call for Safeguards on Medical Disclosure. Is a Federal Law Necessary?* NATIONAL LAW JOURNAL, May 30, 1994, at A1

What Does the Rule Require?

The requirements outlined in the privacy rule are based on many of the practices that already are employed by health care providers and insurers across the country. The rule compiles many of these practices into a single, comprehensive law. Although numerous terms and concepts, such as "patient consent" and "patient authorization," will be familiar throughout the health care industry, the privacy rule redefines many terms and concepts and inserts them into a new framework.

The privacy rule has four basic parts:

1. *Use and disclosure:* An entity may use or disclose identifiable health information only when the rule either requires or allows the use or the disclosure.

2. *Minimum necessary:* When an entity uses or discloses health information (as required or allowed by the rule), it must "make reasonable efforts to limit the . . . information to the minimum necessary to accomplish the intended purpose of the use or disclosure. . . ."[27]

3. *Individual rights:* An entity must respond to and accommodate some new individual rights (see the sidebar on page 46).

4. *Administrative requirements:* An entity must institute certain business practices, such as documenting privacy policies and procedures, designating a privacy officer, providing training for employees, and establishing a system of sanctions for employees who violate privacy policies and procedures.[28]

The first part of the framework, which outlines the required and allowed uses and disclosures, is perhaps the most complicated part of the rule, so it is discussed here in detail. The rule *requires* disclosure in only two instances: first, when DHHS needs information to evaluate an entity's compliance with the rule, and second, when a patient requests a copy of his or her own information (for a discussion of the patient's right to request access to his or her health information, see the sidebar on page 46). The rule *allows* use and disclosure in several instances, which fall into three general categories: (1) use or disclosure for purposes of treatment, payment, and health care operations, (2) use or disclosure with the patient's permission, and (3) use or disclosure without the patient's permission.

Use or Disclosure for Treatment, Payment, and Health Care Operations

The original version of the privacy rule published by the Clinton Administration requires most health care providers to obtain the patient's express permission to use health information for treatment, payment, and health care operations.[29] This type of patient permission is termed "consent" under the rule.[30] For example, a local health department's prenatal clinic would be required to seek a woman's consent before providing her with prenatal care or billing her insurer for that care. The consent also would allow the health department to use the woman's health information for its "health care operations"—a term that is defined broadly to include many of the business practices that require the use of health information, such as quality assurance, credentialing of providers, and other management activities.

This consent requirement may ultimately be eliminated from the final privacy rule. In the suggested revisions published this March, the Bush Administration proposed changes that would allow all covered entities, including health care providers, to use and disclose health information for treatment, payment, and health care operations without obtaining the patient's consent. In proposing the change, DHHS explained that the consent process in the current version of the privacy rule could "potentially interfere with the efficient delivery of health care."[31] In lieu of the consent requirement, DHHS proposes to require covered entities to attempt to obtain a patient's written acknowledgment that he or she received a copy of the entity's notice of privacy practices (for a description of the requirement for a notice of privacy practices, see the sidebar on page 46). For example, under the Bush Administration's proposal, the health department's prenatal clinic would not be required to obtain the woman's consent to use her information for treatment or billing purposes, but it would need to give her a copy of the department's notice of privacy practices and attempt to have her acknowledge receiving the notice by signing a form or a log.

Therefore, regardless of whether the final rule requires a consent or simply an acknowledgment of the notice, covered entities will need to have systems in place for obtaining signatures whenever necessary and maintaining appropriate documentation.

Use or Disclosure with the Patient's Permission

In addition to consent, the privacy rule recognizes three other types of patient permission: authorization, opportunity to opt out, and opportunity to agree or object. Each type applies in different circumstances and comes with its own set of requirements.

Patient *authorization* is required when an entity wants to use or disclose health information in a way that is not otherwise permitted by the privacy rule. A patient may authorize any type of use or disclosure as long as the authorization form is consistent with the detailed format and content requirements contained in the rule. For example, if a school requires students to have physical examinations before participating in school sports, a provider (such as a local health department) would have to obtain an authorization (most likely from the parent or guardian) before sending a copy of the physical examination results to the school.

The last two types of individual permission apply in narrow circumstances and are more informal than authorization. First, a person must be given an *opportunity to opt out* of certain uses or disclosures, such as the entity's use of health information for fund-raising purposes. For example, if a hospital wants to use a list of all its cardiology patients in a mailing to raise money for an expansion of the cardiac care unit, it must include a statement in its materials explaining how a patient may opt out of receiving such fund-raising communications.[32] Second, a person must have an *opportunity to agree or object* when an entity is going to use health information in a facility directory (for example, if a hospital discloses information about a patient's condition to the general public through a patient-information line), disclose information to someone involved in the person's care (for example, a friend or a family member), or disclose information to people or organizations involved in certain disaster relief efforts.[33] The entity may orally inform the person that he or she has the right to object, and the person may orally agree or object to the use or the disclosure.

In Tampa, a public health worker walked away with a computer disk containing the names of 4,000 people who tested positive for HIV. The disks were sent to two newspapers.

From J. Bacon, *AIDS Confidentiality*, USA TODAY, Oct. 10, 1996, at A1

Use or Disclosure without the Patient's Permission

One aspect of the privacy rule that surprises many members of the public is that it allows entities to disclose health information in a wide variety of circumstances without the patient's permission. In drafting the rule, DHHS recognized that "health information is needed to support certain national priority activities" and that "[i]n many cases, the need to obtain authorization for use of health information would create significant obstacles in efforts to fight crime, understand disease, and protect public health."[34] These national priority activities relate to the following:

- Public health
- Victims of abuse, neglect, or domestic violence
- Law enforcement
- Judicial and administrative proceedings
- Health oversight (for example, fraud and abuse investigations, civil rights investigations, and licensure or disciplinary activities)
- Correctional institutions
- Workers' compensation
- Duties of a coroner or a medical examiner
- Organ, eye, or tissue donation
- Research

Many of these activities are the responsibility, in whole or in part, of state and local governments. Although the privacy rule allows entities to share health information with state or local officials for many of these activities, each type of disclosure may have new strings attached.[35] For example, if a health care provider has reasonable cause to believe that an adult with disabilities needs protective services, the provider is currently required by state law to report this information to the county director of social services.[36] The privacy rule allows this reporting but also requires the provider to notify the adult that the report has been or will be made (subject to limited exceptions).[37]

In addition to these listed categories of permissible disclosures, the rule provides broad authority for disclosures that are "necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public."[38] These disclosures must be consistent with applicable law and ethical standards, be made in good faith, and be made to a person reasonably able to prevent or lessen the threat. A mental health provider, for example, might rely on this authority to disclose health information about a dangerous patient to law enforcement authorities or a potential victim.

How Does the Rule Affect Current Laws?

North Carolina has more than one hundred state statutory provisions, plus many more rules, court decisions, and policies, that intersect with the privacy rule in some way. Many covered entities argued that expecting them to comply with a comprehensive federal law *in addition to* all the state laws was unreasonable; therefore the federal privacy rule should preempt (or override) all other privacy laws. Despite this argument, Congress did not provide DHHS with the authority to preempt all other privacy laws.[39] Rather, it established an extraordinarily complicated relationship between the privacy rule and other laws.

The privacy rule promulgated under HIPAA provides more comprehensive safeguards than previous federal and state legislation did for patients' private information, such as records of counseling and therapy.

People often say as a rule of thumb that HIPAA establishes a "federal floor" of privacy protections. In other words, all federal, state, and local privacy laws that are "more stringent" (more protective) than the privacy rule will remain in place.[40] This rule of thumb is accurate to some extent, but many state laws will remain in place whether or not they are more stringent than the privacy rule.

First, the privacy rule "carves out" several categories of laws from preemption—for example, laws that provide for the reporting of disease or injury, child abuse, birth, or death. North Carolina has many laws that fall into one or more of these carve-outs. For example, one statute directs hospitals to keep birth and death records and to make those records available to the state registrar.[41] This statutory provision falls within the carve-out and therefore is not affected by the privacy rule.

Second, the secretary of DHHS may make individualized determinations that a particular law is not preempted because it is necessary for certain stated purposes, such as preventing fraud and abuse.[42]

Third, the most confusing exception to the federal-floor rule of thumb is that the privacy rule specifically leaves in place any law that "requires" a disclosure. A disclosure is "required by law" if it is mandated by a statute, regulation, court-ordered warrant, grand jury subpoena, civil investigative demand, or similar authority.[43] For example, a North Carolina statute requires substance abuse facilities to furnish health information to the commissioner of motor vehicles regarding people who are involuntarily committed for the treatment of alcoholism or drug addiction.[44] This law will likely stay in effect because the disclosure is required by law, even though the general philosophy underlying the privacy rule would require the patient's authorization for such a disclosure.

Given this complex relationship between state and federal law, it is crucial that covered entities and others who need health information to do their work (such as law enforcement officials and health oversight agencies) seek sound legal advice as they work toward an understanding of their rights and obligations.

Conclusion

The requirements of the privacy rule add a new layer to the already complex landscape of health privacy law. The process of understanding the new law and coming into compliance with it will most certainly be resource-intensive and time-consuming. Therefore, if they have not already done so, local governments and covered entities should begin this process as soon as possible. Once the necessary changes have been implemented and staff have been appropriately trained, all the new requirements that are perhaps intimidating at first glance will become second nature.

Notes

The three highlighted quotations in this article are taken from *Medical Privacy Stories*, Health Privacy Project, Inst. for Health Care Research and Policy, Georgetown Univ. (last updated July 12, 2001), available at www.healthprivacy.org/usr_doc/privacystories%2Epdf.

1. *See* GALLUP ORGANIZATION, PUBLIC ATTITUDES TOWARDS MEDICAL PRIVACY (Sept. 2000) (submitted to the Inst. for Health Freedom), available at www.forhealthfreedom.org/Gallupsurvey/IHF-Gallup.html.

2. 42 U.S.C. §§ 1320d–1320d(8) (Administrative Simplification); 45 C.F.R. pts. 160, 164 (2001).

3. 5 U.S.C. § 552a.

4. *See* 42 U.S.C. § 290dd-2; 42 C.F.R. pt. 2 (implementing regulations).

5. *See, e.g.*, 42 U.S.C. § 1396a(a)(7) (requiring each state's medical assistance plan to provide for safeguarding of information of Medicaid applicants and recipients); 42 C.F.R. pt. 431 [implementing 42 U.S.C. § 1396a(a)(7)]; 42 C.F.R. § 422.118 (requiring managed care organizations participating in Medicare to ensure the confidentiality and the accuracy of enrollee records); 42 C.F.R. § 484.10 (establishing as a condition of participation in Medicare a patient's right to confidentiality with respect to medical records maintained by a home health agency).

6. JOY PRITTS ET AL., THE STATE OF HEALTH PRIVACY: AN UNEVEN TERRAIN: A COMPREHENSIVE SURVEY OF STATE HEALTH PRIVACY STATUTES, Health Privacy Project, Inst. for Health Care Research and Policy, Georgetown Univ. (Aug. 8, 1999), available at www.healthprivacy.org/resources.

7. *See* N.C. GEN. STAT. § 58-67-180 (hereinafter G.S.).

8. *See* G.S. 130A-143.

9. *See, e.g.*, American Medical Association, *Fundamental Elements of the Patient-Physician Relationship*, Ethical Opinion E-10.01, Report

of the Council on Ethical and Judicial Affairs of the American Medical Ass'n (Aug. 2001) ("The patient has the right to confidentiality. The physician should not reveal confidential communications or information without the consent of the patient, unless provided for by law or by the need to protect the welfare of the individual or the public interest"), available at www.ama-assn.org/ama/pub/category/2510.html.

10. *See, e.g., Medical Records Confidentiality Act of 1995: Hearing on S. 1360 before the Senate Comm. on Labor and Human Resources*, 104th Cong. (Nov. 14, 1995) (testimony of Janlori Goldman, Deputy Director of the Center for Democracy and Technology), available at www.cdt.org/ testimony/951114 goldman.shtml; Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL LAW REVIEW 451, 516 (1995) (explaining why a uniform federal law is necessary to develop a coherent and viable health information infrastructure).

11. David C. Kibbe, *A Problem-Oriented Approach to the HIPAA Security Standards*, FAMILY PRACTICE MANAGEMENT, July–Aug. 2001, at 37, 38, available at www.aafp.org/fpm.

12. Small health plans have until April 2004 to comply. 45 C.F.R. § 164.534.

13. Modifications to the Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 67 Fed. Reg. 14,776 (Mar. 27, 2002) (hereinafter Modifications); *see also* A. Goldstein, *Medical Privacy Changes Proposed*, WASHINGTON POST, Mar. 22, 2002, at A1.

14. SL 2001-424 (signed Sept. 26, 2001).

15. The privacy rule subdivides covered entities into a few additional categories, including hybrid entities, affiliated covered entities, covered entities with multiple covered functions, and organized health care arrangements. *See* 45 C.F.R. §§ 164.504(b) (discussion of "health care component of a hybrid entity"), 164.504(d) (discussion of "affiliated covered entities"), 164.504(g) (discussion of "covered entities with multiple covered functions"), 164.501 (definition of "organized health care arrangement"); Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,502–09 (Dec. 28, 2000) (hereinafter Privacy Rule Preamble) (preamble discussion and regulation text relating to organizational requirements for different types of covered entities). There are benefits and drawbacks to each category. Compliance officers should review the rule carefully to determine if an entity falls within a special category.

16. HIPAA provides for civil monetary penalties of $100 for each violation (up to $25,000 per year). 42 U.S.C. § 1320d-5(a)(1). Criminal penalties range from a fine of $50,000 and/or up to one year in prison, to a fine of $250,000 and/or up to ten years in prison. 42 U.S.C. § 1320d-6.

17. 45 C.F.R. § 160.203.

18. A social services agency's determining eligibility for Medicaid or Health Choice does not automatically mean that it is a covered entity (i.e., a health plan) or a business associate. The agency also would have to perform other functions that would qualify it, such as providing home health services. Privacy Rule Preamble, 65 Fed. Reg. at 82,479.

19. *Id.* (definition of "health plan," "health care clearinghouse").

20. *Id.* (definition of "business associate").

21. "If covered entities were able to circumvent the requirements of these rules by the simple expedient of contracting out the performance of various functions, these rules would afford no protection to individually identifiable health information and be rendered meaningless." Privacy Rule Preamble, 65 Fed. Reg. at 82,640.

22. This would be true only if no other privacy laws applied to the third party.

23. A covered entity will be held responsible under HIPAA for the misdeeds of a business associate only "if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the [contract] unless the covered entity took reasonable steps to cure the breach or end the violation" and, if such steps were unsuccessful, the entity either terminated the contract or reported the problem to DHHS. 45 C.F.R. § 164.504 (e)(1)(ii).

24. *See* Privacy Rule Preamble, 65 Fed. Reg. at 82,567 ("We agree . . . that comprehensive legislation is necessary to provide full privacy protection and have called for members of Congress to pass such legislation. . . ."); *id.* at 82,641 ("[W]e agree that there are advantages to legislation that directly regulates most entities that use or disclose protected health information. However, we reiterate that our jurisdiction under the statute limits us to regulate only those covered entities listed in § 160.102").

25. *See* Privacy Rule Preamble, 65 Fed. Reg. at 82,618–19.

26. Recognizing that tight restrictions on oral communications could present some implementation challenges, the Bush Administration's proposed revisions include several changes that, if adopted, would provide more flexibility with respect to oral disclosures occurring "incidentally" while the entity is making a disclosure that is otherwise permitted by the privacy rule. *See* Modifications, 67 Fed. Reg. at 14,785–86.

27. 45 C.F.R. § 164.502(b). There are several exceptions to the "minimum necessary" requirement. For example, an entity does not need to limit the information disclosed to health care providers for treatment purposes. *Id.*

28. *Id.* § 164.530.

29. *See* 45 C.F.R. § 164.501 (definitions of "treatment," "payment," and "health care operations").

30. Consent as required by the privacy rule is not the same as the commonly used informed consent. "Informed consent," as it has been interpreted and applied in most instances, refers to a patient agreeing to certain treatment (after adequate discussion and/or disclosure), whereas "consent" required by the privacy rule refers to a patient providing permission to use and disclose information. *See* G.S. 90-21.13 (informed consent to a health care treatment or procedure); *see generally* FAY A. ROZOVSKY, CONSENT TO TREATMENT: A PRACTICAL GUIDE § 1.0 (2d ed., Boston: Little, Brown, 1990, and 2d ed. Supp., Gaithersburg, Md.: Aspen Publishers, 1999). The consent required by the privacy rule is not intended to be uninformed, however. The rule requires that the patient be provided with a "notice of privacy practices," which will provide detailed information on how information will be used and disclosed by the covered entity (see the sidebar on page 46).

31. *Fact Sheet: Standards for Privacy of Individually Identifiable Health Information —Proposed Rule Modification*, DHHS (Mar. 21, 2002), available at www.hhs.gov/news/press/2002pres/20020321.html.

32. 45 C.F.R. § 164.514(e)–(f).

33. 45 C.F.R. § 164.510. Each category of disclosure is subject to certain limited exceptions.

34. Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 59,925 (proposed Nov. 3, 1999) (to be codified at 42 C.F.R. pts. 160, 164) (preamble to the proposed privacy rule).

35. *See* 45 C.F.R. § 164.512 (specifying the rules that apply to disclosures for each type of "national priority activity").

36. G.S. 108A-102 (requiring "any person having reasonable cause to believe that a disabled adult is in need of protective services" to report such information to the director of social services).

37. 45 C.F.R. § 164.512(c).

38. *Id.* § 164.512(k).

39. 42 U.S.C. § 1320d-7.

40. 45 C.F.R. §§ 160.202 (definition of "more stringent"), 160.203 (outlining the general rule of preemption and the exceptions, including the "more stringent" exception).

41. G.S. 130A-117.

42. 45 C.F.R. § 160.203(a). If an exception is granted under this section, it stays in effect until either the secretary revokes it or the state law or the privacy rule changes such that the ground for the exception no longer exists.
45 C.F.R. § 160.205.

43. 45 C.F.R. §§ 164.501 (definition of "required by law"), 164.512(a) (required-by-law exception).

44. G.S. 20-17.1(e).

Privacy and Computer Security: Nine Questions

Kevin FitzGerald

This issue of *Popular Government* has devoted much attention to the legal parameters on sharing and protecting private information. Of equal importance is the security of information technology systems that store and convey sensitive information. This article poses nine straightforward questions for government officials to consider in assessing the security of their systems.

There is little doubt that information technology provides critical support for the delivery of government services. Although direct expenditures for technology often represent less than 2 percent of a local government's budget, the reach of technology extends to practically every government service. It is hard to imagine delivering services without the assistance of computer technology.

Local governments, large and small, support a vast array of computer hardware and software systems. They exchange public and private information via the Internet and a variety of "secure" networks among fellow employees, citizens, clients, and other governments. All expect information systems to do the work they were designed to do, be available when they are needed, and maintain the reliability and the integrity of the information that is contained within them.

The importance of security is heightened, and security is made more difficult, as an increasing number of people connect to public information systems. More and more, citizens and employees expect Web-based access to

Dedicated personnel help keep local government computer systems secure.

The author is the director of the Center for Public Technology at the Institute of Government. Contact him at kfitz@iogmail.iog.unc.edu.

Glossary

Disaster recovery plan: [A] plan maintained for emergency response, backup operations, and post-disaster recovery for an information system (IS), to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Firewall: [A] system designed to defend against unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

Patch: In a computer program, one or more statements inserted to circumvent a problem or to alter temporarily or permanently a usually limited aspect or characteristic of the functioning of the program, e.g., to customize the program for a particular application or environment.

Virus: 1. An unwanted program which places itself into other programs, which are shared among computer systems, and replicates itself. *Note:* A virus is usually manifested by a destructive or disruptive effect on the executable program that it affects. 2. Self-replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence.

Source: Telecom Glossary 2000, maintained by the U.S. National Telecommunications and Information Administration, available at http://www.its.bldrdoc.gov/projects/t1glossary2000/.

numerous public services twenty-four hours a day. Also, the technology supporting these connections is diversifying as many governments invest in applications that rely on high-speed Internet connections and support a wide variety of wired, optical, and wireless equipment.

These developments require a security strategy that keeps pace with change while maintaining the fundamental requirements of data integrity. And make no mistake: there are daily threats to data integrity. The viruses (see the glossary, this page) that recently spread from Europe to every corner of the world, destroying billions of dollars' worth of information and erasing countless files, are a spectacular example of the damage that hackers can cause. The 2001 FBI Computer Crime and Security Survey conducted by the Computer Security Institute ranked computer viruses, improper use of Internet connections, the theft of laptop computers, and unauthorized employee access to computer systems as the top four types of security attacks, with the cost per incident ranging from a few thousand dollars to fifty million.[1]

Clearly this is an issue that local officials cannot avoid. Here are nine questions to guide local governments in assessing their security vulnerabilities and in taking reasonable steps to mitigate unnecessary risk. (For helpful Web sites on computer security, see the sidebar on this page.)

Who in our organization is accountable for the security of information technology?
An organization should designate someone to be responsible and accountable for computer security. This often is a responsibility of the information technology director. The person should have sufficient technical training to do the job.

Do we have an information technology security plan?
There should be a written plan that is periodically reviewed and well communicated to management and employees. It should cover critical data policies, backup, disaster recovery, and user policies.

Helpful Links

Institute of Government, Center for Public Technology
http://www.cpt.unc.edu
The Center for Public Technology is a unit of the Institute of Government. Its mission is to assist North Carolina governments in making use of information technology to improve services and strengthen communities.

Top 20 Internet Security Vulnerabilities
http://www.sans.org/top20.htm
This site contains a listing of and information on twenty of the greatest Internet security vulnerabilities. It is maintained by the SANS (System Administration, Networking, and Security) Institute and the National Infrastructure Protection Center.

State of North Carolina Security Documentation
http://www.its.state.nc.us/Support/Security/Security.asp
This site contains information on the State of North Carolina's security plan. It is maintained by the North Carolina Office of Information Technology Services.

Glossary
http://www.its.bldrdoc.gov/projects/t1glossary2000/
The U.S. National Telecommunications and Information Administration maintains this searchable glossary.

Are our software licenses, patches (see the glossary), and various maintenance agreements up-to-date?
Software, equipment, and networks are continually modified. It is essential that these systems be kept up-to-date. Making sure that security provisions like firewalls (see the glossary) and virus software are current is especially important. A log of updates should be maintained. At times, virus definition files are updated several times a day. Servers and workstations should be set to download updates automatically and install the most current versions.

Is our security plan keeping up with our changing use of technology?
If there has been a recent upgrade in systems that changes traditional network configurations, the assumptions of the security plan must be reexamined to ensure that the plan has not been compromised.

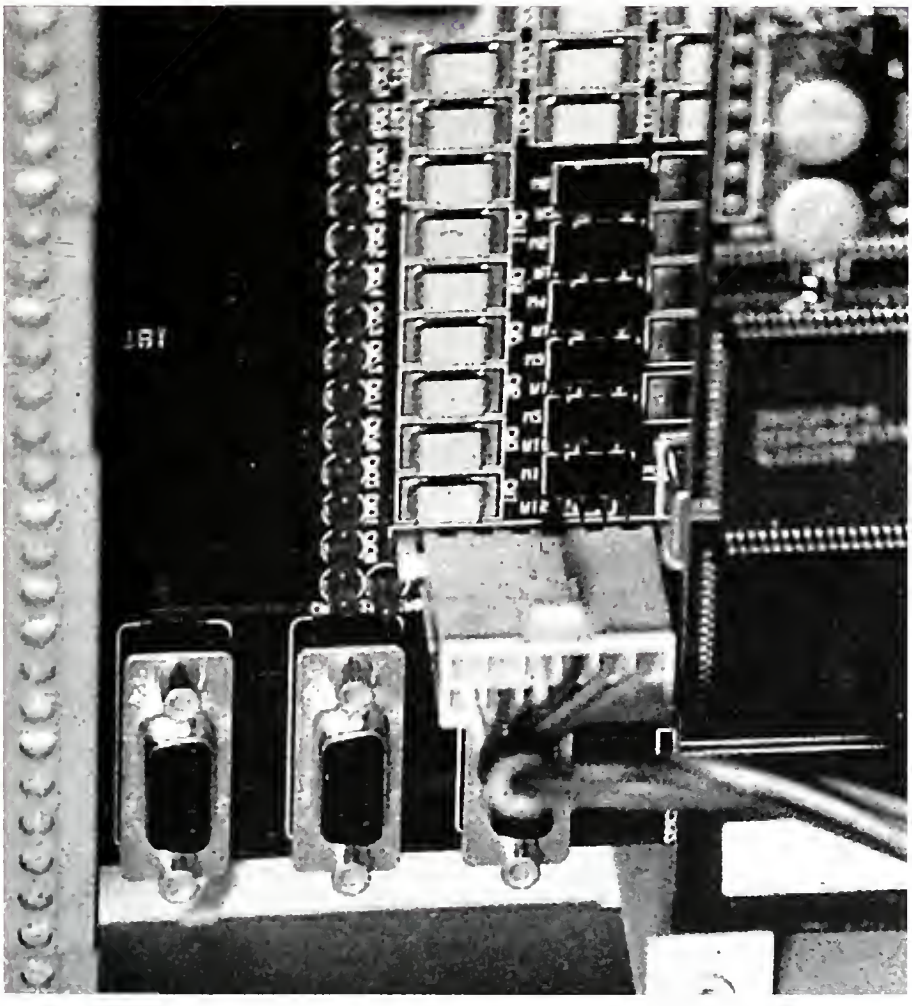
Do we keep valuable equipment locked up?
Theft of equipment, especially laptop computers, can easily compromise sensitive information. Users whose laptops contain sensitive data should consider encrypting their hard drives to reduce the possibility of misuse.

How do we know if a hacker has gotten into our system or if data have been changed?
Software is available that is capable of detecting whether an unauthorized user has crossed the security perimeter. This information is helpful in understanding which systems are particularly vulnerable.

Do we have a disaster recovery plan (see the glossary) that is tested and capable of supporting operations without excessive loss of data?
Suppose a natural disaster destroys a unit's data center. Is the unit capable of restarting operations in a reasonable timeframe? Are backup tapes stored far enough off the site that they would survive a disaster such as a tornado? A government unit should consider negotiating a reciprocal agreement with another unit using the same hardware and software, whereby each would provide the other with emergency processing services.

What steps have we taken to train employees about security? Do employees know what is and is not acceptable behavior? Do they know where and how to report problems?
Clear written policy related to computer use and abuse is essential. This should be included in an employee's orientation.

Are we clear in our communications with citizens and clients about the security and the privacy of the information that is maintained?
Citizen confidence is critical. Citizens need to know what steps are being taken to ensure that private information is kept private.



Conclusion

Identifying what information is private is important. Ensuring that private information remains secure is just as important. Otherwise, privacy, and the confidence that citizens place in the custodians of the private information, may be compromised.

Note

1. 2001 CSI/FBI Computer Crime and Security Survey (San Francisco, Cal.: Computer Security Inst., 2001), available at www.gocsi.com.

Law Firm Makes Lead Gift to Judicial Endowment Fund

The law firm of Womble Carlyle Sandridge & Rice, PLLC, recently announced a lead gift of $50,000 over five years to the Institute of Government Foundation for an endowment to enhance continuing education programs for North Carolina court officials.

The foundation's Campaign for Judicial Excellence seeks to raise at least $500,000 to support special-topic seminars on current issues of importance in the courtroom; an annual Judicial Sentencing Seminar; national speakers for annual conferences; new reference materials in audio, video, and CD-ROM formats; and professional development for faculty members in the Institute of Government's courts program. To date, more than $100,000 has been raised.

The Insritute of Government's courts program, conducted in partnership with the North Carolina Administrative Office of the Courts, currently offers twenty-one professional conferences and seminars (many of which are held several times each year) and numerous professional publications, which serve more than 3,800 judges, magistrates, clerks of court, district attorneys, public defenders, and others throughout the state.

Established in 1876, Womble Carlyle is one of the largest law firms in the mid-Atlantic and southeast regions, with more than 450 lawyers in nine locations, including Charlotte, Greensboro, Raleigh, Research Triangle Park, and Winston-Salem, North Carolina; Atlanta; Greenville, South Carolina; McLean, Virginia; and Washington, D.C. The firm provides legal and technology-based services to regional, national, and international corporations, businesses, agencies, and foundations in a wide range of industries, including manufacturing, transportation, telecommunications, energy, financial services, health care, life sciences, government, education, and technology.

To support this fund for judicial education and the North Carolina courts, send your gift to Institute of Government Foundation—Drennan Judicial Fund, c/o Ann C. Simpson, CB# 3330 Knapp Building, Chapel Hill, NC 27599-3330.

Brown-Graham Joins Z. Smith Reynolds Board

Associate Professor Anita Brown-Graham has joined the thirteen-member Board of Trustees of the Z. Smith Reynolds Foundation, located in Winston-Salem. Brown-Graham is Albert and Gladys Hall Coates Term Associate Professor of Public Law and Government. She specializes in civil liability of public officials and local governments, and housing and community development.

Established more than sixty years ago for the benefit of the people of North Carolina, the foundation now has assets of about $520 million. No other American general-purpose foundation of that size has a mandate to make grants within a single state.

In working to enhance the quality of life in North Carolina, the foundation places a high value on developing new programs. It currently gives special attention to community economic development, the environment, precollegiate education, and issues affecting minorities and women.

Brown Joins Faculty

Maureen Brown will join the School of Government in June as associate professor of public administration and government. She will work primarily with public administration students and local government officials on information technology management issues.

Brown comes to the school from The University of North Carolina at Charlotte, where she taught information systems in public administration, research methods, strategic planning, policy analysis, and program evaluation. She is particularly interested in the use of information-based technologies to promote public and nonprofit initiatives in service delivery. For example, she has worked extensively with the Charlotte-Mecklenburg Police Department on projects to design and manage major technology systems.

As a senior research fellow at George Washington University's Center for Excellence in Municipal Management (Washington, D.C.), Brown also teaches executive-level programs on information systems for municipal leaders and is directing the design and development of an electronic government program for state and local government executives.

Brown received a D.P.A. in 1994 from the University of Georgia. Earlier she earned a B.S. at the University of Maryland and an M.P.A. at the University of Oklahoma.

—Ann C. Simpson

Off the Press

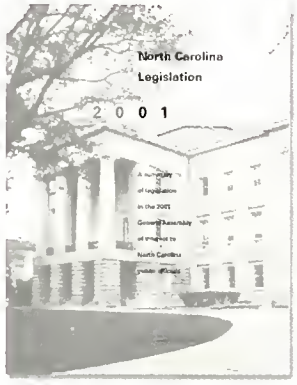
A Legal Guide to Public Employee Free Speech in North Carolina

Stephen Allred
Third edition, 2002 • $15.00*

Examines the legal principles governing the First Amendment right of public employees to speak on matters of public concern and the right of public employers to maintain an efficient workplace. Written to be helpful to lawyers and nonlawyers alike.

North Carolina Legislation 2001: A Summary of Legislation in the 2001 General Assembly of Interest to North Carolina Public Officials

Edited by William A. Campbell
2002 • $40.00*

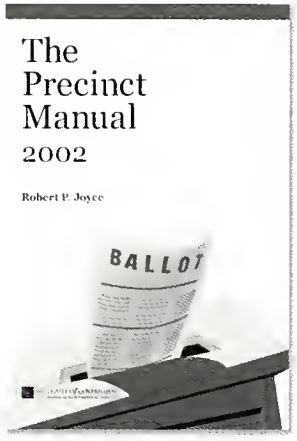


A comprehensive summary of the General Assembly's enactments during the 2001 legislative session, written by Institute faculty members who are experts in the fields affected by the new statutes.

The Precinct Manual 2002

Robert P. Joyce
2002 • $8.00*

Published every two years, this book is a basic introduction to the law governing administration of elections. Used by precinct registrars and judges, it explains North Carolina law on registering voters, conducting elections, counting ballots, and other matters of concern to precinct officials.



Recent Publications

Introduction to Zoning
David W. Owens
Second edition, 2001 • $20.00*

Municipal Benchmarks: Assessing Local Performance and Establishing Community Standards
David N. Ammons
Second edition, 2001 • $59.95*
Published by Sage Publications, Inc.

Suggested Rules of Procedure for the Board of County Commissioners
Joseph S. Ferrell
Third edition, 2002 • $13.00*

ORDERING INFORMATION

Subscribe to *Popular Government* and receive the next four issues for $20.00*

Write to the Publications Sales Office, Institute of Government, CB# 3330, UNC–CH, Chapel Hill, NC 27599-3330

Telephone (919) 966-4119

Fax (919) 962-2707

E-mail sales@iogmail.iog.unc.edu

Web site shopping cart https://iogpubs.iog.unc.edu/

Free catalogs are available on request. Selected articles are available on-line at the Institute's Web site.

To receive an automatic e-mail announcement when new titles are published, join the New Publications Bulletin Board Listserv by visiting https://iogpubs.iog.unc.edu/ and scrolling to the bottom of the page, or view all School of Government listservs at http://www.iog.unc.edu/listservs.htm.

***N.C. residents add 6.5% sales tax.**
Prices include shipping and handling.

Nonprofit Org.
US Postage
PAID
Permit #216
Chapel Hill, NC

Popular Government
(ISSN 0032-4515)
Institute of Government
CB# 3330 Knapp Building
The University of North Carolina at Chapel Hill
Chapel Hill, North Carolina 27599-3330

http://iog.unc.edu