

Report of the Special Directive Subcommittee
to the New Jersey Privacy Study Commission
September 8, 2003

I. INTRODUCTION: The Special Directive

This report responds to Executive Order 26, in which the Governor directed the New Jersey Privacy Study Commission "to study the issue of whether and to what extent the home address and home telephone number of citizens should be made publicly available by public agencies and to report back to the Governor and the Legislature within six months."¹

The Legislature created the New Jersey Privacy Study Commission in the Open Public Records Act, N.J.S.A. 47:1A et seq., to "study the privacy issues raised by the collection, processing, use and dissemination of information by public agencies, in light of the recognized need for openness in government and recommend specific measures, including legislation, the commission may deem appropriate to deal with these issues and safeguard the privacy rights of individuals."²

¹ Executive Order 21, dated August 13, 2002, may be found at the following web site: <http://www.state.nj.us/infobank/circular/eom26.shtml>

² States maintain records spanning an individual's life from birth to death, including records of births, marriages, divorces, professional licenses, voting information, worker's compensation, personnel files (for public employees), property ownership, arrests, victims of crime, criminal and civil court proceedings, and scores of other pieces of information. These records contain personal information including a person's physical description (age, photograph, height, weight, eye color); race, nationality, and gender; family life (children, marital history, divorces, and even intimate details about one's marital relationship); residence, location, and contact information (address, telephone number, value and type of property owned, description of one's home); political activity (political party affiliation, contributions to political groups, frequency of voting); financial condition (bankruptcies, financial information, salary, debts); employment (place of employment, job position salary, sick leave); criminal history (arrests, convictions, traffic citations); health and medical condition (doctor's reports,

II. CURRENT STATUS OF THE LAW

A. The Open Public Records Act (OPRA)

The New Jersey Open Public Records Act (OPRA) favors disclosure of public records. The preamble to OPRA proclaims the public policy of New Jersey to be that “government records shall be readily accessible for inspection, copying, or examination by the citizens of this state.” N.J.S.A. 47:1A-1. Any limitations on the right of access are to be construed in favor of the public’s right of access.³

The preamble goes on to state “a public agency has a responsibility and an obligation to safeguard from public access a citizen’s personal information with which it has been entrusted when disclosure thereof would violate the citizen’s reasonable expectation of privacy.” *Id.* The right of privacy is specifically secondary to the public right to access.

There is no definition of “personal information” in OPRA, and no general exemption for home addresses or publicly listed home telephone numbers.⁴ Information that is protected from disclosure by other state or federal statutes, regulations, or executive orders may not be disclosed under OPRA. N.J.S.A. 47:1A-9. For example,

psychiatrist’s notes, drug prescriptions, diseases and other disorders); and identifying information (mother’s maiden name, Social Security number).

³ OPRA does not limit the common law right of access to government records. N.J.S.A. 47:1A-8. Even if a record cannot be obtained through a standard OPRA request, it may be possible to obtain the record through the courts. See the discussion on pages 3-4 of this report; *Nero v. Hyland*, 76 N.J. 213, 221-222 (1978); *Higg-A-Rella Inc. v. County of Essex*, 141 N.J. 35 (1995); *Home News Publishing v. State*, 144 N.J. 446 (1996).

⁴ By definition, certain other pieces of information are exempted from disclosure, including the “social security number, credit card number, unlisted telephone number or driver license number of any person.” N.J.S.A. 47:1A-1.1. The statute directs records custodians to redact these pieces of information from documents that are disclosed pursuant to OPRA requests. N.J.S.A. 47:1A-5.

OPRA may not be used to obtain the residential home address of an individual who has obtained protection through the Address Confidentiality Program.⁵

D
r
a
f
t

OPRA specifically makes some home address information accessible, such as the residence of crime victims and criminal defendants, in reports of criminal investigations. N.J.S.A. 47:1A-3(b). This provision directs records custodians to consider “the safety of the victim and the victim’s family, and the integrity of any ongoing investigation.” *Id.* It also provides that “where it shall appear that the information requested or to be examined will jeopardize the safety of any investigation in progress or may be otherwise inappropriate to release, such information may be withheld.” *Id.* As in the predecessor statute,⁶ OPRA continues to provide that no criminal convict should be granted access to information about the convict’s victim, including the victim’s home address. N.J.S.A. 47:1A-2.2.

The Special Directive Subcommittee observes an apparent contradiction regarding the accessibility of a crime victim’s home address under OPRA and its exemption from disclosure. Records custodians cannot readily discern whether requestors are criminal convicts, especially in light of the fact that OPRA permits anonymous records requests. To be sure, N.J.S.A. 47A:1-2.2(c) provides that “a custodian shall not comply with an anonymous request for a government record which is protected under the provisions of this section.” For practical purposes, however, records custodians cannot tell whether the individuals identified in the records have ever been victims of crimes.

⁵ See N.J.S.A. 47:4-1 to -6 (Address Confidentiality Program).

⁶ The predecessor to OPRA was known as the “Right to Know Law.” P.L. 1963, c.73 (C.47:1A-1 et seq.). The old statute provided limited access to records that were “required by law to be made, maintained or kept on file.”

Home address and telephone information may be obtained from government records without using OPRA as the avenue for submitting the request. This is an important point because it pertains to a body of case law that has been codified in OPRA.⁷ The courts remain an avenue for obtaining non-public government records. OPRA specifically provides that it is not to be construed to limit this common law right of access to government records. N.J.S.A. 47:1A-8. Accordingly, the common law right to inspect still exists, so long as the documents are government records, the requestor has a good reason to inspect the records, and the requestor's reasons for inspecting the records outweigh the state's interest in confidentiality.⁸

To put it another way, a requestor may obtain government records that would not be available through OPRA. The requestor must ask a court to weigh and balance the competing interests for and against disclosure of the records. Unlike OPRA, the Common Law Right to Know permits the state to inquire into the requestor's reasons for seeking governmental records.⁹

⁷ The case law has historically been known as the "Common Law Right to Know." The common law RTK generally provided broader access to government records, but required a judicial balancing test. The common law tort of invasion of privacy is discussed below at p. 32.

⁸ The Common Law Right to Know generated a substantial body of case law. Some of the leading cases are Nero v. Hyland, 76 N.J. 213, 221-222 (1978); Higg-A-Rella Inc. v. County of Essex, 141 N.J. 35 (1995); Home News Publishing v. State, 144 N.J. 446 (1996).

⁹ The Common Law Right to Know is to be distinguished from the common law tort of invasion of privacy. Most states, including New Jersey, have adopted a system of categorizing four different kinds of "invasions of privacy." The four torts are (1) "public disclosure of private facts," (2) "intrusion," such as hidden videotape cameras; (3) "appropriation," such as the commercial use of someone's name, image or likeness; and (4) "false light" publicity that places someone in a false light in the public eye. Bisbee v. John C. Conover Agency, 186 N.J. Super. 335 (App. Div. 1982); see also 3 Restatement of Torts 2d §652D. In Bisbee, when a real estate broker published a client's home address, the court held there was no tortious invasion of privacy. See discussion p. 32.

B. Executive Orders 21 and 26

The state's treatment of home addresses and telephone numbers has been the subject of debate since OPRA was enacted. Shortly after the new statute came into effect, the Governor issued Executive Order 21, which, among other things, directed public agencies not to disclose home addresses or home telephone numbers.¹⁰ The Order stated "the Open Public Records Act does not afford county and local governments with any means for exempting access to their records, even where the public interest or a citizen's reasonable expectation of privacy would clearly be harmed by disclosure of those records." Executive Order 21 was later amended by Executive Order 26, which restored access to home address information but directed the Privacy Study Commission to analyze the issue.

The Special Directive Subcommittee takes Executive Order 21 to be an expression of the Governor's concern that the people of New Jersey may have a reasonable expectation of privacy in their home addresses and telephone numbers. Executive Order 26 directs the Privacy Study Commission to report on this issue. Accordingly, this report specifically addresses the issue of the "reasonable expectation of privacy."

This report also includes a broader analysis of legal protection for information about the home. This is done for three reasons. First, the Privacy Study Commission has received testimony from witnesses who invoke statutory, common law, and constitutional reasons for protecting and disclosing home addresses and telephone numbers. Second, as a piece of legal terminology, the "reasonable expectation of privacy" is a matter of

¹⁰ Executive Order 21, dated July 8, 2002, may be found at the following web site: <http://www.state.nj.us/infobank/circular/eom21.shtml>

constitutional and common law. Third, other jurisdictions in the United States and abroad have adopted statutes, treaties, and other legal mechanisms for protecting personally identifying information, including home addresses and home telephone numbers.

II. FINDINGS

A. Public Comment on the Special Directive

The Privacy Study Commission held three public hearings, on June 10, 16 and 17, 2003, at locations in northern, southern and central New Jersey. In addition, the Commission has received written comments from organizations and individuals throughout the state. This report is based on written submissions (including e-mails) and live testimony received through July 31, 2003.¹¹


On the subject of home addresses in open public records, the views expressed at the public hearings fall into two broad categories: one asserting that home addresses should not be disclosed under OPRA and the other asserting to the contrary that they should.¹²

1. Arguments Against Disclosing Home Addresses Under OPRA

The comment most frequently received by the Commission in opposition to disclosure of home addresses and home telephone numbers may be stated as follows: “When I give my home address to the government I don’t want the government to give it to anyone else.” Private citizens and organizations invoked a constitutional right to keep

¹¹ The Privacy Study Commission will hold three more public hearings in the Fall of 2003.

¹² Most of the comments received by the Privacy Study Commission confined their remarks to home addresses. The Special Directive Subcommittee presumes that the points of view and courses of reasoning apply to home telephone numbers as well as to home addresses.



home addresses confidential, and asserted a reasonable expectation that their disclosures to the government should go no further.

Academic Expert

Professor Daniel J. Solove, Assistant Professor of Law at Seton Hall Law School in New Jersey, submitted written comments stating that the disclosure of home addresses and telephone numbers under OPRA could potentially be unconstitutional, and would constitute a departure from the federal approach under the Freedom of Information Act.¹³ He described groups of people who have a strong interest in keeping their home addresses confidential (including celebrities, domestic violence victims, stalking victims, witnesses in criminal cases, abortion doctors and police officers), and cited case law from federal and state courts recognizing a state interest in preserving residential privacy.

Professor Solove stated that the United States Supreme Court has recognized a substantial privacy interest in home addresses and phone numbers. Department of Defense v. F.L.R.A., 510 U.S. 487 (1994) (interpreting the Freedom of Information Act and the Privacy Act of 1974). The United States Court of Appeals for the Third Circuit has held that case law “reflect[s] the general understanding that home addresses are entitled to some privacy protection, whether or not so required by statute.” Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999).

Further, Professor Solove stated that if New Jersey were to routinely give out home addresses and phone numbers, it would not only be violating the Constitution (as interpreted by many federal courts of appeal including, most importantly, the Third

¹³ Professor Solove recently published a casebook entitled *Information Privacy Law* (Aspen Publishing, 2003) (with Marc Rotenberg), and has written extensively on the subject.



Circuit), but it would also be repudiating the privacy protections of the federal Freedom of Information Act approach, which is the approach on which most state open public records acts are modeled.¹⁴

American Civil Liberties Union of New Jersey

The American Civil Liberties Union of New Jersey (ACLU-NJ) testified that confidence in government at all levels is best sustained by access to the information necessary to promote the vigorous public discussion that a well-functioning democracy requires. However, when dealing with information that individuals reasonably expect to remain private and unpublished by the government, the ACLU-NJ said there should be a presumption that such information remain confidential unless there is an overriding justification for its disclosure.

To that end, the ACLU-NJ urged special protection for four categories of information: home address, Social Security Number, medical information and financial information.¹⁵ The ACLU-NJ said two exceptions should apply to the confidentiality of home addresses: voter registration records and tax assessment records should be disclosed, whereas all other home address records should remain confidential. As to financial records the ACLU-NJ recommended one exception: the salaries of public employees should remain public.

The ACLU-NJ pointed out that citizens disclose their home addresses because they are compelled to do so by state law and in order to receive basic

¹⁴ See, e.g., McClain v. College Hospital, 99 N.J. 346, 356 (1985) (noting that most state open public records acts are modeled on the federal Freedom of Information Act).

¹⁵ OPRA already specifically exempts Social Security Numbers from disclosure. N.J.S.A. 47:1A-1.1. This report refers to Social Security Numbers for the purpose of summarizing relevant testimony. Medical and financial records are beyond the scope of this report.

D

governmental services. Since they have no choice but to give their home addresses to the government, they should reasonably expect that the government will not re-disclose their addresses to unknown third parties. The ACLU-NJ asserted a right to privacy in one's home address, under both the New Jersey Constitution and the United States Constitution. See Doe v. Poritz, 142 N.J. 1 (1995); Paul P. v. Farmer, 227 F.3d 98, 101 (3d Cir. 2000); Paul P. v. Verniero, 170 F.3d 396 (3d Cir. 1999).

r

The ACLU-NJ urged the Commission to adopt an objective standard to determine whether home addresses and other confidential information should be disclosed under any circumstances. A balancing test, it argued, would put too much discretion into the hands of government officials.

a

The ACLU-NJ recounted a request it received from a domestic violence victim who was alarmed to find her home address on the state's web site of licensed professionals. The ACLU-NJ urged the State of New Jersey to review and assess which government records containing private information should be redacted and which would be appropriate for full public disclosure because they shed light on governmental operations and other issues of public concern.

f

New Jersey Education Association

t

The New Jersey Education Association submitted written testimony stating "in the strongest terms possible, that public school employees have a most reasonable expectation of privacy such that their home address and telephone number should not be subject to disclosure to any member of the public at any time." The NJEA sought

assurances that home addresses and home telephone numbers would not be subject to disclosure under OPRA.

Domestic Violence Victims' Organizations


The New Jersey Coalition for Battered Women submitted a written statement strongly opposing the disclosure of names, addresses, phone numbers and personal information to the general public. "No victim of domestic violence should be impeded in her or his efforts to remain safe from a batterer by the unmonitored disclosure of their contact information by the government." Likewise, the National Network to End Domestic Violence submitted a report via e-mail, criticizing the practice of publishing domestic violence, sexual assault, and family law cases on the Internet.

Municipal Clerk of the Borough of Paramus




One submission, from the Borough Clerk for the Borough of Paramus, described a case of alleged harassment as a result of OPRA. A requester obtained the names and addresses of all members of the Paramus Shade Tree and Park Commission, took photos of their homes and measurements of their properties, and disclosed the information to others. The requestor urged others to contact the members of the Shade Tree and Park Commission on his behalf. The chair of the commission complained. The clerk expressed concern that it would be difficult to attract municipal volunteers "if the public has the ability to reach workers in the public sector for harassment such as this."

Private Citizens

About twenty individuals submitted impassioned pleas for privacy, in written and verbal testimony. Several made the point that when they provide personal information to the government, they expect the information to go no further. Two expressed fears about




identity theft; two inveighed against unwanted solicitations (including “spam”). Three private citizens made specific reference to a federal law that permits disclosure of personal financial information unless a client makes the effort to “opt-out.”¹⁶ One citizen stated that “people do not want people with disabilities as neighbors,” and said that if addresses and phone numbers of residential programs were made available, disabled individuals might be harassed. One individual testified that attorneys were using municipal court records to contact accident and crime victims as prospective clients. Several witnesses stated that the government should disclose no personal information about them.



One witness, apparently by avocation, combs the refuse of government agencies to determine how carefully their confidential files are handled. He held up a document he declared to contain a public employee’s name, title, salary and Social Security Number. His point, colorfully made, was that confidential information should be adequately protected, in practice as well as by statute. Another witness frequently sued for access to governmental records at his own expense. He claimed to have brought more litigation against public agencies “than all the newspapers put together.”

2. Arguments in Favor of Disclosing Home Addresses Under OPRA



A common view of the right to privacy holds that if a piece of information can be found anywhere in the public domain, it should be available from the state through OPRA. For example, if a citizen’s home address can be found in the telephone book,

¹⁶ The Financial Services Modernization Act (“Gramm-Leach-Bliley”), 15 U.S.C. § 6801 (1999) (establishes “notice and opt-out” as the standard for protecting financial privacy). The witnesses that cited it urged New Jersey to adopt “opt-in” as a better standard, stressing that home address information should not be disclosed without the resident’s express consent.

D voter registration records, or property tax records, this view holds that there is no “reasonable expectation of privacy,” and therefore the state should disclose the home address when it appears as part of a government record. As to unlisted telephone numbers, a similar argument is that an online “Google” search of a telephone number may provide a street address corresponding to the number, and possibly even a map for locating the residence.

r
a
f
t
This argument is consistent with ample case law. According to American Jurisprudence, “the right of privacy is held not to be infringed by the publication of matters of public record.” 62A Am. Jur. 2d § 103 (citing cases). The view is also consistent with search-and-seizure law. The United States Supreme Court has held that, under the Fourth Amendment, unless a matter is kept secret, it enjoys no “reasonable expectation of privacy.” For example, although the Court has found a reasonable expectation of privacy within the four walls of the home, e.g., Kyllo v. United States, 533 U.S. 27 (2001) (thermal imaging), it found no reasonable expectation of privacy in sealed, opaque garbage bags discarded by the curb. California v. Greenwood, 486 U.S. 35, 39 (1988).

Commercial Users of Government Records

Another argument in favor of disclosing home addresses is that commercial data mining serves compelling governmental interests. The Commission heard testimony from Reed-Elsevier, the parent company of Lexis-Nexis and largest commercial provider of public records in the United States, urging the Commission not to exempt home addresses from disclosure under OPRA. The databases compiled from public records throughout the 50 states are used for many purposes, including compelling government

interests such as apprehending criminal suspects, locating witnesses to crimes, and child support enforcement. The Direct Marketing Association testified that it needs home addresses for the purpose of providing valued services to existing and potential customers.

New Jersey Foundation for Open Government

The New Jersey Foundation for Open Government (NJFOG) urged the Commission to reject any sweeping ban on disclosures of home addresses. Emphasizing the axiom that free speech, and by extension open public records, are essential for representative democracy, NJFOG argued that to ban the disclosure of home addresses would undermine OPRA, and impair the ability of the news media to do investigative reporting. For example, to redact home addresses “would make it difficult to determine if the Mary Williams who contributed \$1,000 to the county sheriff’s election campaign is the same Mary Williams who billed the sheriff’s department for \$10,000 in consulting fees last year.” NJFOG observed that OPRA has been in effect for a year, and there have been no significant privacy intrusions reported in the media.

Regarding home addresses, NJFOG pointed out that only a minority of states restricts disclosure and, within that minority, home addresses are protected only for discrete groups such as judges and law enforcement officers. NJFOG argued that the disclosure of home addresses is significantly less intrusive than the disclosure of Social Security Numbers, and observed that most people do not seem to attach much value to the privacy of their home addresses since telephone books routinely publish the information.

D

To redact home addresses from public records is a labor-intensive and costly proposition. NJFOG expressed concern that the burden of the expense might be imposed upon requestors. OPRA provides that when requests involve an extraordinary expenditure of time and effort to accommodate the request, the public agency may charge, in addition to the actual cost of duplicating the record, a special service charge that “shall be reasonable.” N.J.S.A. 47:1A-5(c). NJFOG expressed concern that “some records requests that are now considered routine could morph into requests requiring exceptional effort. In some cases, they could be delayed or denied for that reason and others - especially those involving computer records -- could become prohibitively expensive because extra programming would be needed to redact them.” Routine requests could accordingly become prohibitively expensive, and there may be significant delays in disclosure.

r

a

f

Freedom of Information Center

In written testimony, the Freedom of Information Center at the University of Missouri School of Journalism argued that blanket privacy restrictions would impair government accountability.

Society of Professional Journalists

The Society of Professional Journalists submitted e-mail testimony suggesting that to restrict home address information would impair news reporting.

Professional Investigators

The Commission received verbal and written testimony from several professional investigators, who emphasized the value of public records, and home addresses in particular, for performing services related to law enforcement. These services include

t

D investigating insurance fraud, locating witnesses, pursuing deadbeat parents, and performing due diligence for law firms. One professional investigator characterized these services as the “front line for homeland security,” and several others cited demands for employee background checks.

The professional investigators testified they adhered to a voluntary code of professional conduct,¹⁷ and that their licensing required a number of hours of security or police work. Accordingly they characterized themselves as accountable for any misuse of personal information. One professional investigator urged the Commission to determine whether the crime of identity theft arose from the misuse of public records.

Real Property and Title Search Professionals

r
a
f
t
Four real estate title search companies testified that they need home address information for the purpose of facilitating real estate transactions. The purchase and sale of real estate requires extensive review of records that have traditionally been open for public inspection. In the current market, some transactions require 24-hour turnaround. Title search information includes deeds, mortgages, municipal assessment records, municipal taxes and liens, and judgment liens. These records, which contain home addresses, have been public from time immemorial, and these witnesses urged the Commission not to restrict them now.

¹⁷ The self-regulatory framework for the Individual Reference Services Group (IRSG) is outlined in a report to Congress: www.ftc.gov/bcp/privacy/wkshp97/irsdoc1

D A California company, DataTrace, testified that it is building a database from land records it obtains from county clerks’ offices, as well as from tax records and judgment records. The database is to be made available on a subscription basis.¹⁸

r The Commission also heard testimony from the coordinator of Geographic Information Systems in Somerset County. He represented himself as an advocate for access to data, but expressed concerns as a result of his participation in the Open Data Consortium for the Urban Regional Systems Association. Specifically, he expressed concern that OPRA “neglected to address the capabilities of new technology for using data in ways that have not been thought of before.”

Attorneys

a Nine attorneys sent letters opposing any effort to restrict access to home addresses, especially in reports of motor vehicle offenses. The attorneys use the records as a resource for offering their services to prospective clients, locating witnesses and conducting investigations.

Other Comments

f A business agent for the plumbers and pipe fitters’ union said he needed home addresses to uncover cheating by unscrupulous contractors. One witness expressed a desire for home address information in firearms records, so that he could ascertain whether his neighbors owned guns. An individual testified via e-mail that the philosophy of open government compelled the disclosure of home addresses. Another individual pursued an avocation of testing the responsiveness of state agencies in responding to

¹⁸ A separate subcommittee of the New Jersey Privacy Study Commission is studying the issue of commercial use of public records.

OPRA requests, and urged the Commission to resist, on principle, any limits on open government.

B. Other Jurisdictions

All governments collect and use personal information in order to govern.

Government records include data that contain personal information about individuals.

Many of these records have long been open for public inspection.

Democratic governments moderate the need for information with their obligations to be open to the people and accountable to the legislature, and to protect the privacy of individuals. In the United States, these needs are recognized in the federal and state constitutions and in various public laws.

The issue of protecting personal information first rose to prominence in the 1970s, when computers started becoming important tools for government and commercial enterprise. The United States Privacy Protection Study Commission articulated a set of fair information practices to limit the government's use of personally identifiable information. These fair information practices govern the collection, use, disclosure, retention, and disposal of personal information by the government, and have become widely accepted.¹⁹

¹⁹ These guidelines have become the foundation for many privacy laws and codes of practice around the world. See e.g., Fair Credit Reporting Act, 15 U.S.C. § 1681 (1970) (permissible purposes of consumer reports); Privacy Act of 1974, 5 U.S.C. § 552a (1974) (fair information practices for personally identifiable information); New Jersey Information Practices Act, N.J.S.A. 17:23A-1 (1985) (governs HMOs and other insurance entities); Canada's Privacy Act of 1982, R.S.C. 1985, c. P-21. Every state in the European Union has adopted fair information practices as law. The Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection and Privacy of Transborder Flows of Personal Data are available on the OECD web site at www.oecd.org/dsti/sti/it/secur/index.htm.



Principles of Fair Information Practices

Collection Limitation. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject.

Data Quality. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

Purpose Specification. The purposes for which personal data are collected should be specified not later than the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the purpose specification principle except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation. An individual should have the right:

- (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- (b) to have communicated to him, data relating to him (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him;
- (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability. A data controller should be accountable for complying with measures that give effect to the principles stated above.



In addition to adopting these principles of fair information practices, many jurisdictions have enacted specific legislation regarding home addresses:

California. The California Public Records Act prohibits state agencies from disclosing home addresses of crime victims, judges, elected officials, state employees and utility customers. Cal. Gov't Code § 6254.

Home addresses in voter registration records are similarly confidential, and are not permitted to be disclosed. Cal. Gov't Code § 6254.3

The home address, telephone number, occupation, precinct number, and prior registration number provided by people who register to vote may not be released to the public. Journalists, scholars, political researchers, and other government officials may still get the information. Cal. Election Code § 2194.

Telephone companies may not include unlisted telephone numbers on lists they rent, except to collection agencies and law enforcement. Cal. Pub. Util. Code § 2891.1

Anybody renting or distributing a mailing or telephone list must obtain the user's identity and a sample of the solicitation and verify the legitimacy of the business. Users or renters of lists with children's names on them must take special precautions. Cal. Penal Code § 637.9

Colorado. State officials must keep the following records confidential but permit the individual to see his or her own file: medical and personnel files, library material, and the address and phone number of public school students. Colo. Rev. Stat. § 24-72-204(3)(a) and 24-90-119.

Florida. The Florida "Sunshine" law creates a general and very strong presumption in favor of disclosure of government records. It has no corresponding privacy statute; instead it lists some 500 exceptions to the general rule of disclosure, including exceptions as to the home addresses of specific groups: law enforcement personnel, firefighters, judges, state attorneys, managers of local government agencies, crime victims, government employees, and the spouses and children of individuals in these groups. Fla. Stat. Ann § 119.07.

Every state agency must audit and purge its publication mailing lists biennially by giving addressees the opportunity to continue or to stop receipt of the publications. Fla. Stat. Ann. § 283.28.

Illinois. Motor vehicle and driver license information may not be released to persons without a specific business reason, and there is a ten-day waiting period. Home addresses may not be released if a person has a court order of protection. The law also allows a person to "opt-out" of rentals of DMV lists for commercial mailings

and requires mailing firms to disclose how they will use the lists they procure. 624 ILCS 5/2-123.

Indiana. Each state agency is required to “refrain from preparing lists of the names and addresses of individuals for commercial or charitable solicitation purposes except as expressly authorized by law or [the public records] committee.” Ind. Code Ann. 4-1-6.2

Kansas. Most sales of state lists, including motor vehicle records, are prohibited. Kans. Stat. Ann. §§ 21-3914 and 74-2012.

Montana. State agencies may not rent or exchange mailing lists without the consent of the persons on the lists, except to other state agencies. Voting and motor vehicle records not included. Law enforcement not included. Individuals may compile their own lists from publicly available documents, and certain schools may use lists of license applicants. Mont. Code Ann. § 2-6-109.

Vermont. Lists compiled by public agencies, with exceptions, may not be disclosed if that would violate a person’s right to privacy or would produce private gain. Vt. Stat. Ann. title 1 § 317(10).

Washington. “The work and home addresses, other than the city of residence, of a person shall remain undisclosed” by state agencies if a person says in writing that disclosure would endanger life, physical safety, or property. Wash. Rev. Code Ann. § 42.17.310 (1) (BB).

Voter registration lists are not to be used for commercial purposes. Wash. Rev. Code Ann. § 29.04.100.

Wisconsin. A state or local agency may not sell or rent lists with home addresses unless specifically authorized by statute. Wisc. Stat. Ann. Subch. IV, Ch. 19.

The Federal Election Campaign Act requires political candidates for federal office to record one’s name and address with any contribution for \$50 or more, and occupation and principal place of business once contributions to any one campaign exceed \$100. This information is available for public inspection, although the law prohibits use of the information by others for fund-raising or commercial purposes. 2 U.S.C. 438.

C. Policy Alternatives

The Special Directive Subcommittee has identified a range of policy options for the Commission’s consideration. They are as follows:

D

1. Maintain the Status Quo. The Legislature could do nothing at this time, monitor OPRA requests, and leave policy making to case law and the Government Records Council. This option would be consistent with the empirical observation that the Privacy Study Commission has received only one complaint of an alleged invasion of privacy since OPRA took effect.²⁰

r

2. Remedial Legislation. The Legislature could consider a number of specific revisions to OPRA, such as:

- define “personal information” and charge records custodians with the responsibility to ensure that personal information is not released to the public;
- require public agencies to adopt procedural rules for handling personal information such as giving notice to citizens that their disclosures to the government will become public, giving affected persons a chance to opt-in or opt-out of public disclosure, and redacting personal data from records before the records are published;
- identify a set of data items to be redacted from every record released to the public, such as home address, home telephone number, financial and medical information. The Special Directive Subcommittee notes that if applied to current and historical records, this option would be very burdensome for records custodians. As noted in the specific recommendations below, it may be possible to program computers so that the designated items will not be disclosed in the future;
- identify categories of records to be exempted from public disclosure, such as records concerning minor children;
- identify sets of records as to which home address information would be kept confidential (or disclosed), such as applications for fishing licenses.

a

f

t

3. Enact Specific Privacy Legislation. The federal government enacted the Privacy Act of 1974 as a companion bill to the Freedom of Information Act, and the

²⁰ The complaint, regarding the Paramus Shade Tree and Park Commission, is described above at p. 10.

Supreme Court has interpreted the statutes together. The New Jersey Legislature could similarly enact specific privacy legislation to accompany OPRA.

4. Enact an Omnibus Fair Information Practices Act. Such legislation could require all public agencies to (1) compile an index of all records containing personal information;²¹ (2) permit individuals access to the personal information collected about them that is subject to disclosure; and (3) provide individuals the opportunity to verify the accuracy of that personal information maintained by the agency.

5. Institutional Changes. The Legislature could initiate a number of institutional adjustments, such as giving the Government Records Council power to investigate complaints of invasion of privacy. Additionally or separately, the Legislature could initiate a major institutional change, such as establishing the Privacy Study Commission as a permanent entity, to serve as an ombudsman for privacy issues in New Jersey.

IV. RECOMMENDATIONS OF THE SPECIAL DIRECTIVE SUBCOMMITTEE

A. Legal Analysis and Discussion

1. Special Status of the Home. The Special Directive Subcommittee observes that the home has long enjoyed significant legal protection as a private place. The maxim that “a man’s home is his castle” appeared as early as 1499.²² Parliamentarian William

²¹ The Division of Archives and Records Management (DARM) of the Department of State has an index or registry of all records and corresponding retention schedules maintained by every state and local government agency. The Chief of the Bureau of Records Management, Albin Wagner, has suggested that this registry could be adopted to serve as the “index” suggested in this policy alternative and recommendation 3(b) on p. 38.

²² Solove and Rotenberg, *Information Privacy Law* at 585 (Aspen 2003).

D Pitt wrote, “The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; the roof may shake; the wind may blow through it; the storms may enter; the rain may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.”²³ The Supreme Court recognized in 1886 the importance of protecting “the sanctity of a man’s home.”²⁴ “In none is the zone of privacy more clearly defined when bounded by the unambiguous physical dimensions of an individual’s home.”²⁵

r
a
f
t

The home enjoys a special status as refuge from intrusions by the state and commercial enterprise. See, e.g., Rowan v. United States Post Office Dep’t, 397 U.S. 728, 737 (1970) (individuals have a right to reject unwanted mailings, based upon Congress’s desire to protect the privacy of the home); Fed. Labor Relations Auth. v. Dep’t of Navy, 966 F.2d 747, 756 (3d Cir. 1992) (en banc) (disclosure of an individual’s home address infringes upon a recognized privacy interest); Fed. Labor Relations Auth. v. Dep’t of Treasury, 884 F.2d 1446, 1453 (D.C. Cir. 1989), cert. denied, 493 U.S. 1055 (1990) (Privacy Act prohibits release of home addresses); Nat’l Ass’n of Retired Fed. Employees v. Horner, 879 F.2d 873 (D.C. Cir. 1989) (zero legitimate interest in disclosing home addresses of retired or disabled federal employees).

One of the most famous formulations of the right to privacy calls it “the right to be let alone - the most comprehensive of rights and the right most valued by civilized men.” Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). In Rowan, the U.S. Supreme Court held that the “right to be let alone” in one’s home

²³ Speech on the Excise bill, 1763.

²⁴ Boyd v. United States, 116 U.S. 616 (1886).

²⁵ Payton v. New York, 445 U.S. 573, 589 (1980).

D

requires upholding, against First Amendment challenges, the rights of homeowners to take their names and addresses off various mailing lists:

We ... categorically reject the argument that a vendor has a right under the constitution or otherwise to send unwanted material into the home of another.... That we are often “captives” outside the sanctuary of the home and subject to objectionable speech and other sound does not mean we must be captives everywhere.... The asserted right of a mailer, we repeat, stops at the outer boundary of every person’s domain.” Rowan, 397 U.S. at 738.

r

Rowan places the right to be let alone in one’s home “in the scales with the [constitutionally-protected] rights of others to communicate.” 397 U.S. at 736.

a

Additionally, the Fourth Amendment protects, as against the government, “the right of the people to be secure in their persons, houses, papers and effects,” the Third Amendment protects the home from military use, and the First Amendment protects free expression in the home. See Stanley v. Georgia, 394 U.S. 557 (1969). The Due Process clause of the Fourteenth Amendment specifically protects private conduct in the home.

f

Lawrence v. Texas, 123 S. Ct. 2472, 156 L.Ed.2d 508 (2003).²⁶

Therefore, the Special Directive Subcommittee believes the United States Constitution explicitly protects the home as a refuge from governmental action, and that this protection extends to the disclosure of home addresses and home telephone numbers.²⁷

t

²⁶ Many Supreme Court cases make the point, in a variety of contexts, that the home is the last refuge of privacy. See, e.g., Kyllo v. United States, 533 U.S. 27 (2001) (thermal imaging); Frisby v. Schultz, 487 U.S. 474 (1988) (residential picketing); FCC v. Pacifica, 438 U.S. 726 (1978) (broadcast media).

²⁷ One member of the Subcommittee disagrees with this assertion, on the ground that legal authorities to date have dealt with compilations of personal information, rather than access merely to home addresses. The Subcommittee member asserts that home address information, by itself, does not enjoy constitutional protection.

2. An Individual's Reasonable Expectation of Privacy.

Every individual in New Jersey is compelled to disclose personal information to the government. In order to receive government services, in order to do business with the government, and in order to be a law-abiding citizen, one must provide one's home address and telephone number (listed or unlisted) to the government.

The preamble to OPRA states, in part, "a public agency has a responsibility and an obligation to safeguard from public access a citizen's personal information with which it has been entrusted when disclosure thereof would violate the citizen's reasonable expectation of privacy." The Special Directive Subcommittee interprets this provision to be a substantive one, directing public agencies not to disclose home addresses and telephone numbers if citizens have a reasonable expectation of privacy at the time they disclose this information to the government.

This interpretation is consistent with the constitutional interest in protecting home address information, as articulated by the New Jersey Supreme Court and the United States Court of Appeals for the Third Circuit. It is also consistent with the federal Freedom of Information Act, upon which many open public records statutes are modeled.

a. Constitutional Support. The New Jersey Supreme Court and the United States Court of Appeals for the Third Circuit (the federal court that governs New Jersey) have held that citizens have a constitutional right to privacy in their home addresses.

The New Jersey Supreme Court observed that the "[d]isclosure of a plaintiff's home address, particularly when coupled with the other information disclosed, implicates a privacy interest." Doe v. Poritz, 142 N.J. 1, 84 (1995).

[T]he question of whether an individual has a privacy interest in his or her bare address does not fully frame the issue. The more meaningful

question is whether inclusion of the address in the context of the particular requested record raises significant privacy concerns, for example because the inclusion of the address can invite unsolicited contact or intrusion based on the additional information.

Id. at 83.

The Third Circuit embraces the constitutional right to information privacy, and it has held that there are privacy interests in home addresses. See Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999) (holding that case law "reflect[s] the general understanding that home addresses are entitled to some privacy protection, whether or not so required by a statute"). Even sex offenders have a "non-trivial" privacy interest in their home addresses. Paul P. v. Farmer, 227 F.3d 98, 101 (3d Cir. 2000). See also A.A. v. New Jersey, 2003 U.S. App. Lexis 16853 (3d Cir. August 18, 2003) (sex offenders' privacy interest in home address is substantially outweighed by the state's interest in protecting the public).

In United States v. Westinghouse Electric Corp., 638 F.2d 570 (3d Cir. 1980), the court described a balancing test to determine whether an individual's interest in privacy outweighs the public interest in disclosure:

The factors which should be considered in deciding whether an intrusion into an individual's privacy is justified are the type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.

Id. at 578.

Therefore, the Special Directive Subcommittee believes that in some cases, disclosure of home addresses under OPRA may violate a constitutionally protected right

D to privacy.²⁸ This would occur if an individual’s interest in confidentiality outweighed the government’s interest in disclosure, but a public agency nevertheless disclosed the information.²⁹

b. The Federal Approach. The federal Freedom of Information Act (FOIA), 5 U.S.C. § 552, was enacted in 1966 and amended in 1974. It creates procedures whereby any member of the public may obtain records of the agencies of the federal government. It has served as the model for most open public records statutes in the states.


r
a
f
t
Although the goal of FOIA is full disclosure of government records, Congress concluded that some confidentiality is necessary for the government to function. A federal agency can refuse to release certain types of information. There are nine legal categories that are exempted from FOIA under section 552(b) of the law.³⁰ One category of exemptions is for “private matters.” Another category of exemptions is for “other statutes,” including the federal Privacy Act of 1974.

The Privacy Act of 1974, 5 U.S.C. § 552a, permits individuals to obtain their own records, gives them the right to correct, amend or delete information about themselves,


²⁸ Improper disclosure of information by the government is a recognized injury. See, e.g., Greidinger v. Davis, 988 F.2d 1344 (4th Cir. 1993) (voter registration system found to be unconstitutional because it required voters to disclose their Social Security Numbers publicly in order to vote).

²⁹ Professor Solove cited cases from other jurisdictions in which the constitutional interest in residential privacy was held to outweigh the 6th Amendment right of confrontation. See, e.g., Montez v. Superior Court, 5 Cal.App.4th 763, 7 Cal.Rptr.2d 76 (1992) (home addresses of witnesses); People v. Ramirez, 55 Cal.App.4th 47, 56-57, 64 Cal.Rptr.2d 9 (1997) (name of anonymous victim); People v. Lewis, 184 Cal. Rptr. 31 (Cal. Ct. App. 1982) (home addresses of arresting police officers); but see Reid v. Superior Court, 55 Cal.App.4th 1326, 1329, 1336-1339, 64 Cal.Rptr.2d 714 (1997).


³⁰ The exemptions are for (1) national security; (2) internal agency rules; (3) other statutes; (4) business information; (5) internal government memos; (6) private matters; (7) law enforcement investigations; (8) regulation of financial institutions; (9) oil wells.




and gives them the right to sue federal agencies if they refuse to correct or amend the records. The default provision of the Privacy Act is that records regarding personal individuals will not be disclosed.




The New Jersey Supreme Court has looked to FOIA and the Privacy Act for guidance in cases interpreting the old Right To Know statute and the Common Law Right to Know. See, e.g., Higg-A-Rella, Inc. v. County of Essex, 141 N.J. 35, 50 (1995); McClain v. College Hospital, 99 N.J. 346, 356 (1985). Likewise, the Special Directive Subcommittee looks to the court decisions interpreting these statutes for guidance in discerning the “reasonable expectation of privacy” as articulated in OPRA.



Reading FOIA and the Privacy Act together, the U.S. Supreme Court has said that individuals have a reasonable expectation of privacy with respect to their home addresses. In United States Dep’t of Defense v. Fair Labor Relations Authority, 510 U.S. 487 (1994), the Court explained:



It is true that home addresses are publicly available through sources such as telephone directories and voter registration lists, but in an organized society, there are few facts that are not at one time or another divulged to another. ... An individual’s interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information is made available to the public in some form.... Id. at 500. “We are reluctant to disparage the privacy of the home, which is accorded special consideration in our Constitution, laws and traditions.” Id. at 501.



This is consistent with ordinary experience. In New Jersey, many people have a reasonable expectation that their home addresses will be private. These include children and individuals who have made a genuine effort to keep their home addresses private, by securing unlisted telephone numbers or asking to be removed from mailing lists.

Professor Solove identified other groups of people who often seek protection of their

home address information: celebrities, domestic violence victims, stalking victims, witnesses in criminal cases, abortion doctors, and police officers.

D If an individual does not want his or her residence to be known, the importance of its being unknown goes to the core of his or her individual privacy. People who do not want their home addresses released have limited means for preventing disclosure, and little recourse once the disclosure has been made. The Special Directive Subcommittee does not believe it is the state government's intention to force individuals to sacrifice their privacy as a condition of doing business with the government.³¹

r
a But the potential for invasion of privacy is exacerbated by the increased reliance on technology in governmental administration. Until recently, public records were difficult to access. Finding information about an individual often involved making personal visits to local offices to locate records. But in electronic form, public records can be easily obtained and searched from anywhere. Once scattered about the country, public records are now often consolidated by commercial entities into gigantic databases.

f The Special Directive Subcommittee believes it may violate an individual's reasonable expectation of privacy if the government discloses information to the public that would otherwise be unobtainable. Especially serious are examples of government records that contain sensitive personal information. For example, municipal recreation

t³¹ To some extent, New Jersey has recognized an obligation to protect privacy for some individuals. The Address Confidentiality Program, N.J.S.A. 47:4-1 et seq., allows victims of domestic violence to use an alternate address for all state and local governmental purposes, including driver's licenses and registration, professional licensing, banking and insurance records, welfare, etc. New Jersey laws also enable victims of domestic violence to vote without revealing their addresses, N.J.S.A. 19:31-3.2. Victims of sexual assault and stalking may use an alternate address on their driver's license and registration. N.J.S.A. 39:3-4.

department records may include personal information about children, such as birth dates, emergency phone numbers, and medical conditions.

The courts recognize a privacy interest every time the government discloses an individual's home address, even when the disclosure results in only a minimal effect, such as unsolicited contact. See e.g., Dep't of Defense, 510 U.S. at 500-501. The government has a duty to protect the privacy interests of individuals who have taken steps to protect themselves. This is true despite, and indeed because of, the technological advances that have made individuals vulnerable to unwarranted intrusions from the commercial sector.

c. Non-Governmental Sources of Home Address Information. Under OPRA, it is the government, rather than commercial enterprise, disclosing information about individuals. This makes a difference.³² An individual's home address may be found in a telephone book or on the Internet, but this fact does not justify action by the government to disclose the same home address when the individual held a reasonable expectation of privacy at the time he or she gave the information to the government.

Many people do not care if their addresses are published, but for some it can be a matter of life or death. Professor Solove cited the murder of Rebecca Shaffer, who was killed by a stalker who got her address from motor vehicle records. The fact that some - or even most - people allow their home addresses to be published by commercial entities does not mean that the government should disclose the same information. As the Third Circuit explained:

³² See Kinsella v. Welch, 362 N.J. Super. 143, 157, 827 A.2d 325 (App. Div. 2003) (explaining distinction between the constitutional right of privacy (which pertains to government action) and its common law namesake (which pertains to non-governmental action)).

D

The compilation of home addresses in widely available telephone directories might suggest a consensus that these addresses are not considered private were it not for the fact that a significant number of persons, ranging from public officials and performers to just ordinary folk, choose to list their telephones privately, because they regard their home addresses to be private information. Indeed, their view is supported by decisions holding that home addresses are entitled to privacy under FOIA, which exempts from disclosure personal files “the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.”

r

Paul P. v. Farmer, 227 F.3d 98, 101 (3d Cir. 2000) (quoting the Freedom of Information Act, 5 U.S.C. § 552(b)(6)). See also Remsburg v. Docusearch, 149 N.H. 148, 816 A.2d 1001 (2003) (stalker case).

a

Moreover, just because a piece of information is in a “public record” doesn’t mean it can be published for any purpose. As the U.S. Supreme Court explained in United States Dep’t of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989):

f

“[There is a] privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public.” Id. at 767. “The compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of information. The dissemination of that composite of information infringes upon both the common law and the literal understandings of privacy [that] encompass the individual’s control of information concerning his or her person.” Id. at 763. “Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a [government-created] computerized summary located in a single clearinghouse of information.” Id. at 764. “[T]he fact that an event is not wholly ‘private’ does not mean that an individual has no interest in limiting disclosure or dissemination of the information.” Id. at 770.

t

The Special Directive Subcommittee agrees that generally the public should not have access to home addresses if the primary effect of the disclosure would be solely the dissemination of personal information about an individual, without such disclosure

D shedding light on the conduct of a public agency or official or on other governmental matters of significance to the public.

d. **The Common Law Tort of “Invasion of Privacy.”** Most states, including New Jersey, have adopted a system of categorizing four different kinds of “invasions of privacy.” The four torts are (1) “public disclosure of private facts;” (2) “intrusion,” such as hidden videotape cameras; (3) “appropriation,” such as the commercial use of someone’s name, image or likeness; and (4) “false light” publicity that places someone in a false light in the public eye. Bisbee v. John C. Conover Agency, 186 N.J. Super. 335 (App. Div. 1982) (no tortious invasion of privacy where real estate broker published a client’s home address); 3 Restatement of Torts 2d §652D.

a
f
The tort of invasion of privacy differs substantially in its origins from the line of cases following the constitutional right to information privacy and FOIA-type statutes.³³ In Bisbee, the information was not disclosed by the government, so the case is not as pertinent to OPRA as the cases that speak to governmental action.

A crucial distinction between the constitutional right of privacy and its common law namesake is that the common law right operates as a control on private behavior, while the constitutional right operates as a control on government. The two rights are necessarily different because our concept of appropriate behavior for private persons and government officials is different.

Kinsella v. Welch, 362 N.J. Super. 143, 157, 827 A.2d 325 (App. Div. 2003)

(brackets and internal citations omitted).

³³ The tort was first proposed by Louis Brandeis and Samuel Warren in a very famous 1890 law review article: *The Right to Privacy*, 4 *Harvard L. Rev.* 193 (1890). The constitutional right to information privacy was first articulated by the United States Supreme Court in Whalen v. Roe, 429 U.S. 599 (1977).

3. Unfunded Mandates and Exposure to Litigation.

The Special Directive Subcommittee acknowledges the burdensome nature of redacting home addresses from paper records. Redaction is labor intensive, time consuming and costly.

In the future, it may be cost effective to program government computers not to disclose home addresses and telephone numbers. The Subcommittee assumes that most OPRA requests in the future will ask for electronic copies of electronic records. Many current and old records are still on paper however, and most are archived and difficult to access. Some OPRA requests are for dozens of boxes or thousands of documents stored at remote locations or in media that are difficult to retrieve.

OPRA directs records custodians to redact Social Security Numbers, unlisted phone numbers, credit card and driver license numbers. N.J.S.A. 47:1A-5. The Subcommittee is inclined to believe that home addresses and telephone numbers appear more often in government records, potentially increasing the burden on custodians to redact them. Many state and local government agencies may lack the resources to respond promptly to OPRA requests because they have inadequate retrieval systems or inadequate staff to perform the necessary redactions.

Who will pay for these kinds of requests? OPRA provides that public agencies may impose a “special service charge” for requests that involve “an extraordinary expenditure of time and effort.” N.J.S.A. 47:1A-5(c). Some local government agencies have claimed they should be entitled to charge for any request that takes more than 15 minutes to process. The New Jersey Superior Court rejected the 15-minute criterion in Courier Post v. Lenape Regional High School District, 360 N.J. Super. 191 (2002), and

offered instead the following factors to be considered to determine whether an OPRA request should be considered “extraordinary”:


1. the volume of government records involved;
2. the period of time over which the records were received by the government unit;
3. whether some or all of the records sought are archived;
4. the amount of time required for a government employee to locate, retrieve and assemble the documents for inspection or copying;
5. the amount of time, if any, required to be expended by government employees to monitor the inspection or examination; and
6. the amount of time required to return the documents to their original storage space.

Id. at 199.

The Special Directive Subcommittee agrees with the court that ordinary OPRA requests should not be transformed into “extraordinary” requests, which might then become prohibitively expensive for requestors. The Subcommittee believes as a general proposition that the expense of redacting home addresses should not be borne by requestors but should instead be considered part of the cost of providing governmental services.³⁴




This proposition places a very significant burden on public agencies. OPRA is not an unconstitutional unfunded mandate. See Courier Post, 360 N.J. Super. at 207, citing N.J. Const. Art. VIII, Sec. 2, Par. 5 (effective December 7, 1995) and N.J.S.A. 52:13H-1 et seq. (Local Mandates). Nevertheless, the cost is very real and may be staggering for local governments, in staff time, technical equipment, and workspace.

³⁴ Cf. Eric Neisser, Charging for Free Speech, 74 Geo. L. J. 257 (1985).




By the same token, litigation is burdensome and costly. Public agencies, including local governments, may be exposed to lawsuits if the agencies improperly disclose home addresses, violating the constitutionally protected right to individual privacy.

B. Specific Recommendations of the Special Directive Subcommittee



The Special Directive Subcommittee believes the core purpose of the New Jersey Open Public Records Act (OPRA), N.J.S.A. 47:1A et seq., is to enhance public understanding of the operations and activities of government. Official information that sheds light on a state agency's performance of its statutory duties falls squarely within that statutory purpose. That purpose, however, is not fostered by disclosure of information about private citizens that is accumulated in various governmental files but that reveals little or nothing about an agency's own conduct. See DOD, 510 U.S. at 495-96, quoting Reporters Committee, 489 U.S. at 773, and Dep't of Air Force v. Rose, 425 U.S. 352, 360-361 (1976).



Accordingly, the Legislature should evaluate the reasons public agencies collect and disclose home addresses and telephone numbers. There are legitimate reasons for collecting and disclosing this kind of information. However, disclosure may in some instances be unwarranted. The Special Directive Subcommittee proposes the following recommendations as a way to balance the public's recognized need for openness in government while safeguarding the privacy rights of individuals.



1. Public agencies should notify the public, whenever appropriate, that home addresses and telephone numbers may become public.

Many people are unaware that their home addresses and telephone numbers may become public when they give this information to state and local government agencies. For example, if they have an “unlisted” telephone number, they may not expect their addresses and phone numbers to be disclosed pursuant to an OPRA request. Several witnesses testified that when they give information about themselves to the government, they expect it to go no further.

Accordingly, the Special Directive Subcommittee recommends that the Legislature require public agencies to provide notice that such information may be disclosed.



2. Home Telephone Numbers Should Be Kept Confidential.

Records custodians have no way to tell whether the home telephone numbers in government files are listed or unlisted. This means that for practical purposes, it is difficult for the custodians to comply with the provisions of OPRA that direct them to redact unlisted telephone numbers.

The Special Directive Subcommittee recommends that records custodians act with an abundance of caution and treat all home telephone numbers as confidential. This will not harm requestors, because the requestors can use other sources like telephone directories to obtain listed numbers.



3. The Legislature Should Identify Categories of Government Records that Should Be Kept Confidential, and Provide Objective Guidelines to Records Custodians

The Special Directive Subcommittee believes that the citizens of New Jersey have a reasonable expectation of privacy in their home addresses and telephone numbers.³⁵

Generally, the Subcommittee also believes it would be desirable in many cases to inquire into a requestor's reasons for seeking home addresses and telephone numbers. There exists no viable mechanism for doing this, however.³⁶ OPRA does not permit records custodians to make such inquiries, and the Special Directive Subcommittee believes records custodians should not be given discretion to prefer one request over another.

Records custodians need clear, neutral guidelines to determine whether or not a record should be disclosed under OPRA. The Special Directive Subcommittee has identified two strategies for developing such guidelines.

a.) Identify Categories of Individuals. The Legislature should exempt certain groups, such as judges and law enforcement officers, where there are demonstrable safety risks to the members of those groups.³⁷

³⁵ Most members of the Subcommittee consider the “reasonable expectation of privacy” to be a substantive provision of OPRA. One member disagrees, however, on two grounds. First, the preamble may be taken as a legislative finding, describing the interests weighed by the Legislature in the process of enacting OPRA, not as a separate exemption for personal information. Second, no case law to date deals with the question of access to home address information by itself. The legal authorities cited in this report analyze home address information packaged together with other data to reveal more than mere home addresses in isolation.

³⁶ The only mechanism currently available to engage in a balancing test is the Common Law Right to Know, described above at p. 4. The Special Directive Subcommittee views litigation as an unduly burdensome obstacle for most requestors.

³⁷ For example, judges and law enforcement officers may be targets of retaliation. This option does not account for the safety interests of individuals unless they are members of an exempt group.

D

Of special concern to the Subcommittee are the home addresses of crime victims. The Special Directive Subcommittee recommends that N.J.S.A. 47:1A-3(b) be amended to provide disclosure only of the victim's city of residence.³⁸

r

b.) Identify Categories of Records. The Division of Archives and Records Management in the Department of State maintains an index of the repositories of information maintained by public agencies in New Jersey.³⁹ Some repositories, such as medical records, are already exempt from disclosure. The Legislature should identify additional repositories from which home address information should similarly be exempted by statute.

a

The Division of Archives and Records Management compilation could be used as a register of the records created, received and maintained by every state and local government agency in the State of New Jersey, along with retention schedules and other record keeping requirements established and approved by the State Records Committee.

f

The register would indicate whether the records contain personal or confidential information that would have to be restricted, and whether access to the records should be restricted because of state or federal statutes.⁴⁰

t

³⁸ One member of the Special Directive Subcommittee dissents from this recommendation, for two reasons. First, people have a right to know about crimes that have taken place in their neighborhoods, so that they can take steps to protect themselves. Second, OPRA incorporates the provisions of Executive Order 123, which was signed by Governor Kean and widely accepted.

³⁹ An incomplete but illustrative list of open public records is attached as an appendix to this report.

⁴⁰ The Special Directive Subcommittee acknowledges that to evaluate every database in the DARM index would be a tremendous achievement.

The Special Directive Subcommittee recommends that the Legislature consider several factors to determine whether home addresses should be exempted:⁴¹

- the type of record requested;
- the potential for harm in any subsequent nonconsensual disclosure;
- the injury from disclosure to the relationship in which the record was generated;
- the adequacy of safeguards to prevent unauthorized disclosure;
- the degree of need for access;
- whether there is an express statutory mandate, articulated public policy or other recognizable interest militating toward access.

4. Public Agencies Should Program Their Computers to Collect but Not Disclose Home Address and Home Telephone Information.

Every new and upgraded computer system should be designed so that, where appropriate, the data fields for home addresses and telephone numbers can be flagged as non-disclosable and automatically removed from the record when OPRA requests are filled by public agencies. The Special Directive Subcommittee believes that in the future, most OPRA requests will be answered in electronic form, making systems design a technological answer to safeguarding an individual's reasonable expectation of privacy.

⁴¹ These factors are enumerated in United States v. Westinghouse Electric Corp., 638 F.2d 570 (3d Cir. 1980). The Westinghouse case is discussed at greater length above at p. 26.

Appendix
Incomplete but Illustrative List of Open Public Records

D

Appeals of government agency decisions
Arrest reports
Autopsy reports (including coroners reports)
Bank records (e.g., management of city bond funds; records to determine the condition and viability of banks and other financial institutions; determine status of government involvement with private banks)
Budgets (to monitor government revenue collection and spending at all levels)
Business records (to monitor government oversight of regulated businesses)
Cameras (generalized surveillance)
Campus crime and disciplinary records
Census information
Contracts (including proposals and bids)
Death certificates
Driving records, including violations and arrests
Election records, including campaign finance
Environmental cleanup
Expense records
Financial records of government agencies
Geographic information systems
Governor's schedules, staff, expenses and travel
Health inspections (eg NY public school cafeterias)
Highway contracts
Highway safety
Hospitals
Jails
Labor negotiations (collective bargaining)
Law enforcement
Legislative records and meetings
Marriage licenses and applications
Meeting notices, agendas and minutes
Nursing homes
Personnel records
Photographs
Prisons and corrections systems
Public schools
Real estate appraisals
Regulatory boards and agencies
School testing data
Vital statistics, including birth records, to track population and demographic trends
Voting, including registrations, ballots and equipment
Zoning and community planning

r

a

f

t

Worker safety records
Union contracts
Utility records