

FINAL REPORT

PRIVACY STUDY COMMISSION

**Submitted to Governor Richard J. Codey
and
The New Jersey State Legislature**

December 2004

December 31, 2004

The Honorable Richard J. Codey, Acting Governor
Senator Richard J. Codey, President of the Senate
Assemblyman Albio Sires, Speaker of the General Assembly

Dear Acting Governor and Members of the Legislature:

On behalf of the New Jersey Privacy Study Commission, I am pleased to present to you the Commission's report on the privacy concerns and protection recommendations.

The Commission prepared this report pursuant to the Legislature's charge in N.J.S.A. 47A:1A-1 et. seq., establishing a Privacy Study Commission "...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"; and Governor McGreevey's mandate in Executive Order 26 to study the issue of whether and to what extent the home addresses and home telephone numbers of citizens should be made publicly available by public agencies. This report is the culmination of the Commission's consideration of public comment, as well as statutory and judicial analysis on the issue.

The Commission believes that the policy recommendations for administrative and legislative action contained in this report strike an appropriate balance between the needs for openness and the transparency of government and the citizens' reasonable expectation of privacy in their personal information contained in government records. Further, it is the Commission's belief that its findings and recommendations will be useful to both the executive and legislative branches of government in New Jersey, as well as serve the best interest of the citizens of New Jersey.

Sincerely,

M. Larry Litwin, APR
Chair, New Jersey Privacy Study Commission

Final Report

Table of Contents

Subject	Page #
Transmittal	i
Preface	v
Commission Membership	vii
Executive Summary	1
Introduction	5
Section 1: Privacy And The Impact Of Technology	7
Section 2. Report On Home Addresses And Telephone Numbers	15
Section 3: Report On Commercial Use	47
Section 4: Data Practices Survey	69
Section 5: Conclusion	89
Appendix A	91
Appendix B	99

Preface

Remarks of M. Larry Litwin, APR Chair, New Jersey Privacy Study Commission

The time has come for me, as chair, to thank every member of the Commission for their dedicated service as we worked hard to research, debate, recommend and adopt a number of reports that are the framework for a final report to be sent to the Acting Governor and then . . . on to the Legislature.

The Privacy Study Commission was created under the Open Public Records Act (OPRA) to study the privacy issues raised by the collection, processing, use and dissemination of information by public agencies – balancing the recognized need for openness in government with concerns for personal privacy and security.

Over nearly two years, all of us participated to study the privacy issues in light of the recognized need for openness in government – while, at the same time – protecting the privacy rights of individuals.

As charged by the Governor, we studied home addresses and telephone numbers, the use of personal information by commercial entities for title searches, mortgage and other loan applications, and information used by private investigators and other firms that use personal information for such publications as printed and on-line directories. We spent a great deal of time studying technology and its effect on the way government operates.

We are making specific recommendations that we deem appropriate to strike a balance between openness in government and . . . protecting the individual.

We appreciate all the assistance of staff members, Marc Pfeiffer, Paul Dice, Susan Jacobucci and Erin Mallon Knoedler, but especially, early on – Catherine Starghill – who compiled a matrix consisting of legislation in every state and ranked them by effectiveness. I could not place a value on Catherine’s help.

In drafting, debating and adopting our reports, we reviewed the collection, processing, use and dissemination of information by State and local government agencies here in New Jersey and in many other states.

My personal objective was for us to work together – as a Commission – so that we would achieve the overall goal of striking that balance between an individual’s right to privacy and the public’s right to know. It was a major challenge – one this commission has met.

Thank you to all of the chairs – Grayson Barber for chairing the Special Directive Committee on Home Addresses and Telephone Numbers . . . and for presenting a document that met with unanimous approval . . . Tom Cafferty for his work as chair of the Commercial Use Committee and Bill Kearns for chairing the Technology Committee.

Judge Karcher-Reavey chaired the Public Interest Committee, which handled the public hearings and made recommendations for the web site. Also, Karen Sutcliffe for chairing the Committee on New Jersey Practices and Ms. Barber, again, for chairing the Committee on Practices Outside of New Jersey.

While they are the chairs, none of our work could have been completed without the input of George Cevasco, Richard DeAngelis, Edithe Fulton, John Hutchison, Pamela McCauley, Jack McEntee and Lawrence Wilson.

And, thank you to any DCA staff members I may have missed. Thank you to Commissioner Susan Bass Levin for the confidence she has shown in us . . . and my personal thanks to Tara Bennett, the Rowan University graduate who served as my intern.

While our final report may not be perfect in everyone’s eyes, I see it as a benchmark that other states could emulate.

It has been an honor to serve as Commission chair.

NEW JERSEY PRIVACY STUDY COMMISSION

MEMBERS

M. Larry Litwin (Chair)
Rosemary Karcher Reavey
Grayson Barber
Thomas Cafferty
George Cevasco
Richard DeAngelis, Jr.
Edithe A. Fulton
John Hutchison
William John Kearns, Jr.
Jack McEntee
Pamela McCauley
Karen Sutcliffe
H. Lawrence Wilson

Executive Summary

An individual's right to privacy as balanced with an open and transparent government has been at the forefront of common law and statutory open public records debate in New Jersey.

The Privacy Study Commission was created as a result of the enactment of the Open Public Records Act, N.J.S.A. 47A:1A-1 *et seq.* [OPRA]. OPRA favors disclosure of public records, yet the Act also states that public agencies have a responsibility to safeguard personal information when disclosure would violate a citizen's reasonable expectation of privacy.

The Privacy Commission studied three (3) specific areas: the disclosure of home addresses and telephone numbers; commercial use of public information held by public agencies; and the impact of technology on privacy concerns. Further, the Commission conducted a New Jersey Data Practices Survey. The full reports of these subjects areas and the survey are contained within. The reports also offered specific recommendations that are summarized below.

General Recommendations

- The Legislature should establish a permanent entity to serve as an ombudsman for privacy issues in New Jersey.
- The Legislature should provide a source of adequate funding to comply with Open Public Records Act ("OPRA") requests, so as to not unduly burden either requestors or records custodians with the expense of searching records, redactions and other requirements. Guidelines need to be developed on what constitutes an "extraordinary expense" under OPRA.
- The State should administer a "New Jersey Data Practices Survey" on a periodic basis.
- Public agencies should only collect the data they need to serve their statutorily mandated functions and refrain from collecting extraneous personal information.
- Public agencies should provide individuals with the opportunity to verify the accuracy of their personal information maintained by the agencies.
- Public agencies should notify the public that the information provided on official forms may be disclosed, unless otherwise exempt by law.
- Public agencies should program their computer systems and applications to collect, but not disclose information exempt from access as provided by law.

Privacy and the Impact of Technology

- E-mail addresses provided by individuals to government entities should be accorded the same protection as unlisted phone numbers, i.e., they should remain confidential.
- There should be thorough and mandatory training provided for all of those who have custody of government records, not just the formally designated Custodian of Records, on the impact of technology and the steps that are necessary to be taken in order to protect the authorized confidential information when records are provided to a requestor in electronic format.
- The training, and any equipment required to implement privacy protection of electronic data should be provided by the State of New Jersey as a State expense and should not be left to local government entities to provide as their limited resources will allow.
- New Jersey should establish an Office of Privacy, which would work with, and, perhaps, within the Office of Information Technology to be able to interact and to assist in identification of privacy related issues and to bring those issues to the attention of those charged with determining the appropriate boundaries for access to government records, such as the Government Records Council or the Courts.
- When agencies adopt regulations establishing certain records as not subject to disclosure, those agencies need to recognize the impact of technology on the ability to search records and to make the regulations comprehensive enough to ensure that the regulation making certain records not subject to disclosure are not evaded by the use of technology.

Home Addresses and Telephone Numbers

- Home telephone numbers, including cell phone numbers, should not be disclosed.
- Public agencies should notify individuals that their home addresses might be disclosed pursuant to OPRA requests.
- Individuals should be permitted to provide an address of record for disclosure purposes, in addition to their home address when interacting with public agencies.
- The Governor or Legislature should establish objective guidelines defining when and from which government records home addresses should be redacted.
- Individuals should be permitted to opt out of disclosure of their home addresses.
- In the future, computer systems and applications should be programmed to collect but not disclose home addresses and telephone numbers.

Commercial Use of Government Records

- The Legislature has addressed privacy concerns through exemptions in OPRA and other statutes, such as worker's compensation and insurance laws. It has also left the door open for other exemptions through regulations, further legislation and executive order of the Governor. Exemptions from access for the commercial use of information should be contained in legislation, regulations or by Executive Order of the Governor.
- The Legislature and/or the Governor should consider abuses arising from the commercial use of information, such as data-mining, as well as the benefits of access, such as aiding local businesses. Along with transparency of government comes the responsibility to safeguard citizens' reasonable expectation of privacy.
- The Legislature and/or the Governor should be mindful that any restrictions deriving from secondary or derivative uses of records that may be deemed abusive cannot and should not result in legislation restricting access, but rather, such legislation should be directed at the perceived abuse either by increasing punishment, if present punishment is inadequate, or enacting legislation defining additional actions that will be deemed abusive and imposing punishment therefore.
- The Legislature and/or Governor should consider the proposition that when the secondary or derivative use of a public record is a commercial/profit-making use, the commercial user should be expected to contribute to the cost recovery of developing and maintaining such records. Those who advocate such a position recommend that such a fee should be likened to a user fee with those gaining financially from the use of public records helping to pay a portion of the development and maintenance costs. Other states, however, have declined to impose such a "user fee" noting that the statutory right of access should not be perceived as a revenue generating mechanism.

Data Practices Survey

In an effort to determine and track the data practices of state and local government units and agencies, especially as it relates to the handling of personal information, the New Jersey Privacy Study Commission recommends that a scientifically developed and monitored data practices survey be administered every two years to a mandatory response population of state and local government units and agencies by the Department of State – Division of Archives and Records Management (DARM) or the Privacy Study Commission if this organization is adopted by the Governor or legislature as a permanent entity. The Commission believes that in doing so, the state will become better informed of how state and local government units and agencies are adhering to the policy in OPRA requiring that public agencies safeguard citizens' personal information with which they are entrusted. Further, this mandatory survey may motivate agencies that are not in compliance with OPRA's policy to safeguard personal information from public access to do so.

Introduction

The Open Public Records Act, N.J.S.A. 47:1A-1 *et seq.* (Chapter 404, P.L. 2001), created the Privacy Study Commission 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.”

The Privacy Study Commission, through Executive Order 26 (dated August 12, 2002), was directed by the Governor to, “...promptly study the issue of whether and to what extent the home addresses and telephone number of citizens should be disclosed by public agencies in the state...”

The Commission consists of thirteen (13) members appointed by the President of the Senate (1 member), the Minority Leader of the Senate (1 member), the Speaker of the General Assembly (1 member), the Minority Leader of the General Assembly (1 member) and the Governor (9 members). In addition to the study of home addresses and telephone numbers of citizens, the Commission also specifically studied the secondary use of government records by businesses and entities other than government [Commercial Use report]; Privacy and the Impact of Technology [Technology Report]; and also conducted a New Jersey Data Practices Survey.

The Commission met, generally on a monthly basis, throughout a two-year period and formed sub-committees to study specific areas of privacy concerns. The sub-committees submitted reports that were accepted and voted on by the Commission. The compilation and finalization of these reports are hereby submitted to the Governor and the Legislation in fulfillment of the Privacy Commission’s designated charge.

Section 1: Privacy and the Impact of Technology

Technology has developed at a rapid pace, and will continue to develop in the future, without regard for policies regarding appropriate use of that technology and the protection of the privacy interests of the people who are impacted by the technology based access to what is reasonably considered to be private information.

It is for that very reason that it is critically important to develop policies to manage and control the application of technology in order to respect the privacy interests of citizens.

The very concept of privacy is a matter of extensive public debate. In October 2000, Presidential candidate George W. Bush said, “I believe that privacy is a fundamental right and that every American should have absolute control over his or her personal information.”¹

Since then, concerns over homeland security have caused government to accumulate a broad range of personal information on individuals. That information rests in electronic databases, along with private information accumulated in the normal conduct of governmental activities as people register for government programs, obtain licenses and permits, enroll in schools, register for electronic toll passes, go to government related web sites, etc. The increasing use of technology has a very significant impact on the ease with which those outside the government can access the accumulated data.

In the name of homeland security, there were proposals that the Federal government initiate a “Total Information Awareness” project to accumulate personal records from banks, medical files, credit card companies, schools, etc. and combine them into a master data base. The public reaction was instant and very public, with an outcry resulting in Congress taking action to block the funding for the project.²

Prior to the development of massive databases of information, there was a natural limit on the intrusiveness of information maintained in government records. The use of paper-based records made the accumulation of the data and the cross-referencing of the data very labor intensive.

The technology revolution of the past decade and the cost effectiveness of computer based searching technologies, combined with the adoption of technology to maintain a

¹ *Privacy in Retreat*. An article by William Safire in the New York Times, March 10, 2004.

² *Privacy Invasion Curtailed*. *New York Times*. February 13, 2003.

full range of governmental records presents both an opportunity for easy use by governmental entities for valid governmental purposes as well as the serious potential for abuse of the information.

The cross-referencing of records of electrical permits, dog licenses and senior-citizen tax records, for example, carry serious security implications. Cross-referencing those records could easily reveal properties where there are no alarm systems, no dogs and are occupied by elderly or disabled residents. Such cross-referencing is easy with the technology-based records, but was virtually impossible when those records were all maintained only in a paper format. Easy access to electronic records of registrations for recreation programs with the names, addresses, phone numbers, etc. of juvenile registrants should be a basis for concern by parents and by the government custodians of that sensitive information.

Data base information about which houses in town are vacant, records of hospital admissions³, requests to police to watch particular properties, requests to suspend delivery services for short period of time, etc. should all be treated as private and not subject to disclosure. Federal legislation has barred **commercial** web sites from collecting information on children up to the age of 12, but that legislation does not address governmental web sites. At the very least, similar protections should be applied to New Jersey governmental web sites. Action should be taken by legislation or regulation to provide that the release of personal identifiable information, such as addresses, phone numbers, e-mail addresses, gathered through governmental web sites is prohibited.

As GIS (Geographic Information System) programs develop at every level of government providing the cross-referencing of multiple information databases, it becomes critically important to develop statewide policies on privacy in order to avoid a hodgepodge of policies at state, county, municipal, authority, school district and agency levels.

There is a cost involved in applying privacy policies to data. Some governmental entities have taken an easy course in making everything available because of the cost involved in developing, applying and maintaining data where various classifications are treated as private.

Where a governmental entity or employee, such as a Tax Assessor, Health Inspector, Police Commander, may have a need for access to a broad range of information, that need does not automatically translate into making that same information available to anyone with a computer and the ability to surf the Internet.

While citizens generally are comfortable with providing information to their government, an astounding 72% have only some or very little trust in the government to use that

³ Many hospital records are protected with regard to confidentiality by reason of federal law (HIPAA) that requires certain patient specific information to be treated with confidentiality. To the extent of the federal law, OPRA also treats that information as confidential.

information properly.⁴ The manner in which government handles information that citizens regard as private will most certainly impact on the broader issue of whether citizens can trust their government at all.

The public reaction to the use of technology to cross-reference data became evident in 2003 when the news came out that an internet search engine, Google, made it possible to enter a telephone number, perform a search and have the name and address of the individual come up on the screen. A further click provided a map showing where the person was located.⁵ When the news broke, people flocked to the Google web site to exercise the option to make their information private.⁶

Another issue that needs to be considered arises in situations where government entities contract out with private companies for the development, management and maintenance of data. Once that data becomes available to the private company, there is no system, no regulation, and no law to prevent that company from making the data available on a commercial basis. Government entities are enticed to the public-private partnership in the development of the technology and the database simply because of the cost involved. The private partner in the process can make the service available to government at a very low cost; precisely to gain access to the data that has a significant commercial and resale value.

It is easy to suggest that certain categories of information should be isolated from database information and should not be accessible. The implementation of such a recommendation is, however, problematic.

While the State of New Jersey and many county governments have well staffed and knowledgeable information technology departments, that is simply not the case for other levels of governments, including municipalities, school districts and authorities.

There is a need for technology support, especially for local governments in the securing of protected data. While the State has a substantial Information Technology staff to address issues, that same level of support is virtually non-existent at the local government level. When a request is received for data in electronic format, the local custodians of records⁷ do not have the technical expertise to make sure that when the data is copied the fields that are private are effectively deleted and not copied as part of the record. Both training and equipment are needed. This results in a very substantial cost impact. Where privacy is identified as a matter of significant importance, the protection of the privacy

⁴ *From the Home Front to the Front Lines: America Speaks Out About Homeland Security*. Council for Excellence in Government, March, 2004, page 7.

⁵ *Another Online Privacy Intrusion*. *Philadelphia Inquirer*, March 29, 2003.

⁶ *Some Search Results Hit Too Close to Home*. *New York Times*. April 13, 2003.

⁷ For municipalities, the Custodian of Records, specified by the Open Public Records Law, is the Municipal Clerk. For other local entities, the official Custodian of Records is designated by the local entity.

should not be thwarted by the unavailability of the technical support required to protect that privacy.⁸

Many of those levels of government have the records being maintained by individuals who are trained in the use of computers for specific purposes, but not in the underlying technology involved. While the individual might be able to set up a database with a field that does not appear on the screen of someone simply accessing the data at a terminal in the governmental office, there is a very serious potential for breaching privacy when the individual seeking the information requests the data in an electronic format.

The simple act of copying the database to a disk for someone does not mean that the protections built in to the database to prevent certain fields from showing up will be preserved. Anyone with a basic knowledge of databases can simply go into the management aspects of the database and remove the commands that block the visibility of the hidden fields. There must be a serious and effective effort to prevent that from happening.

Municipalities, school districts and authorities simply do not have the technical capacity to address those issues and do not have the financial resources to establish that information technology management resource.

Effective protection of privacy for the information that is either currently mandated by law to be treated as private or that becomes classified as private as the result of the work of the Privacy Study Commission will require intensive training and allocation of resources. It will require significant funding and sharing of technology resources by the State with the local governmental entities.

E-Mail address lists are developed when citizens give a municipality or county or state agency an e-mail address in order to receive notifications of specific information, Those individuals do not anticipating that the e-mail address list will be made available to anyone who asks for it so that advertising and other types of unwanted spam can be sent out. E-mail addresses should be treated in the same manner as unlisted telephone numbers, i.e., they should not be made available.

Every State has a library confidentiality law⁹ that prevents the dissemination of information on borrowers. The Privacy Study Commission acknowledges those protections and reaffirms that records of library usage, including internet access, should be treated as private and not be treated as a public record.¹⁰ It is noted that the Federal

⁸ It should be remembered that when the State mandates certain actions and expenditures by local governments, the State may be required to provide the funding for those mandates under the State Mandate-State Pay amendment to the New Jersey State Constitution, Article VIII, Section II, Paragraph 5, and the implementing legislation, *N.J.S.A. 52:13H-1, et seq.*

⁹ *N.J.S.A. 18A:73-43.2*

¹⁰ Library confidentiality laws are being challenged in the State of Michigan where a law student has demanded that 85 libraries across the state turn over records on patron names, addresses, telephone numbers and e-mail addresses. The demand has been made under the provisions of the Michigan Freedom of Information Act, notwithstanding the library confidentiality law. *Detroit News, July 6, 2004.*

Video Privacy Protection Act bars the release of video rental records. That legislation was enacted after the Senate confirmation hearings in 1987 on the nomination of Robert Bork to the Supreme Court, when records of video rentals by Mr. Bork were obtained and released. Those records came from a private video rental company, but the same principle applies to libraries that make a wide range of materials available to borrowers.

Information in governmental records regarding the location of alarm systems, surveillance cameras, etc. should be clearly and unequivocally classified as security information and should be treated as confidential. To fail to do so would be to assist potential law violators.¹¹

Technology is being used in law enforcement efforts, including such technologies as “Red Light Cameras” that take pictures of vehicles at intersections. Other surveillance cameras are used at arenas, parking garages and other locations where security is important or simply where there is a perceived need to watch what employees are doing.¹² Surveillance records (to extent they include information about persons not targets of the surveillance) -- example: a video tape of drivers exceeding posted speed limit should not be available to public to demonstrate who the driver had accompanying him or her in the car.

Financial transactions with government offices are increasingly being accomplished with the use of credit and debit cards. That transactional information should be classified as private and all information relating to the user, the card numbers, expiration dates, etc. should be fully protected from any public access.

The Commission has learned of certain regulations that direct local Registrars of Vital Statistics to strictly limit the availability of certified copies of certain records, but that regulation did not address uncertified copies of records or the copying of entire databases of those records of births, marriages and deaths. The salutary purpose of the basic regulation can be easily undermined because the regulation is insufficiently comprehensive.

While e-mail records are being treated throughout the country as the equivalent of letters, there is no guidance on how to maintain those records, the cost involved in archiving, the means and cost involved in retrieving the records, the means to distinguish between the e-mail messages that should be fully public and those that are personal and private. In Florida, it is the employee who makes the determination as to which e-mail records are personal and which are business related. While OPRA is intended to apply to records that have been “made, maintained, or kept on file in accordance of his or its official

¹¹ It should be noted that language in OPRA does require that security measures and surveillance techniques are not subject to disclosure. That language is in the process of being supplemented and clarified by Regulations proposed by the Attorney General that are in the public comment period as this report is being prepared.

¹² New Jersey Transit has installed hidden video cameras on its trains as a safeguard against theft. Cameras are also installed in some train stations. Those cameras, however, also tape transit employees along with the passengers who are on the trains and that surveillance raises privacy issues. *Cameras Upset Riders and Crew. New York Times.* March 6, 2004.

business,” there is a need for clear guidelines to be established to identify the e-mail records that need to be archived, how to accomplish that task and to provide the resources to make that possible.

In the field of public contracts, we are rapidly moving toward the maintenance of the records of bids in an electronic format. Responses from bidders may frequently include financial data that is used to enable the government to evaluate whether the bidder is able to undertake and perform the contract involved. That financial data needs to be safeguarded, since the release of it would give other bidders (on future contracts) a significant advantage by knowing the financial capacity, indebtedness, resources, of their competition. That would reduce the competitive nature of the public bidding. Additionally, obtaining details from unsuccessful bidders would enable other bidders to know in which areas they could increase their bids without fear of the competition. Again, that would defeat the very purpose of public bidding. While OPRA does provide an exemption for that information, the challenge in maintaining that information in an electronic format is that the confidentiality is not as easily protected as when the information is only in paper-based format. The ability to comply with the confidentiality requirements in a technology based record retention system requires both training and the hardware-software needed to prevent that information from improperly being accessed by others.

Technology is a boon for cost-effective management of data in private businesses as well as in government offices. The drive to obtain the benefits of technology, however, cannot ignore the impact that the technology has on privacy and on the rights of citizens to have confidence that their government is not the ultimate culprit in the dissemination of their private information.

Any effort to expand the use of technology must include the development of effective means to maintain the privacy of information that is deemed to be private and it is the obligation of the State to provide the technical and financial resources to accomplish that level of protection for government entities at all levels, State, County, Municipal, School District and other governmental authorities.

New Jersey should have a structured Office of Privacy, which would work with, and, perhaps, within the Office of Information Technology to be able to interact and to assist in identification of privacy related issues.

Recommendations:

In the area of the impact of technology on privacy issues relating to governmental records, the Privacy Study Commission recommends that:

1. E-Mail addresses provided by individuals to government entities should be accorded the same protection as unlisted phone numbers, i.e., they should remain confidential.
2. There should be thorough and mandatory training provided for all of those who have custody of government records, not just the formally designated Custodian of

Records, on the impact of technology and the steps that are necessary to be taken in order to protect the authorized confidential information when records are provided to a requestor in electronic format.

3. The training, and any equipment required to implement privacy protection of electronic data should be provided by the State of New Jersey as a State expense and should not be left to local government entities to provide as their limited resources will allow.

New Jersey should establish an Office of Privacy, which would work with, and, perhaps, within the Office of Information Technology to be able to interact and to assist in identification of privacy related issues and to bring those issues to the attention of those charged with determining the appropriate boundaries for access to government records, such as the Government Records Council or the Courts.

When agencies adopt regulations establishing certain records as not subject to disclosure, those agencies need to recognize the impact of technology on the ability to search records and to make the regulations comprehensive enough to ensure that the regulation making certain records not subject to disclosure are not evaded by the use of technology.

SECTION 2: REPORT ON HOME ADDRESSES AND TELEPHONE NUMBERS

Executive Summary

The disclosure of home addresses and telephone numbers contained in government records is at the forefront of the privacy debate in New Jersey. While the New Jersey Open Public Records Act favors disclosure of government records, it also states that public agencies have a responsibility to safeguard personal information when disclosure would violate a citizen's reasonable expectation of privacy.

In light of the concern over the disclosure of home addresses and telephone numbers, the New Jersey Privacy Study Commission was given the special directive to review this issue and develop recommendations before concluding on the Commission's general task of studying the privacy issues raised by state and local government's collection, processing, use and dissemination of information under OPRA.

The Commission created the Special Directive Subcommittee to specifically study whether and to what extent home addresses and telephone numbers should be disclosed by public agencies in the state. In doing so, the Subcommittee considered the arguments for and against disclosure set forth by the public at open hearings held throughout the state. Comments were received from academic experts, representatives of state and local government, the American Civil Liberties Union, organizations for open government, organizations of education professionals, victims' organizations, press organizations, commercial resellers of government records, professional investigators, attorneys and private citizens.

The Subcommittee also considered legislation enacted by other states that have specifically addressed the issue of public disclosure of home addresses and telephone numbers as examples of legislative frameworks currently in place throughout the country. Additionally, the Subcommittee reviewed the statutory interpretations of an individual's reasonable expectation of privacy regarding the disclosure of home addresses and telephone numbers in the federal Freedom of Information Act and the Privacy Act of 1974. Further, the Subcommittee considered the judicial interpretations of the same provided by the U.S. Supreme Court, U.S. Court of Appeals for the Third Circuit, and the New Jersey Supreme Court as the Subcommittee developed its policy recommendations on this issue.

In accordance with its special directive, the New Jersey Privacy Study Commission developed the following recommendations for consideration by Governor McGreevey and the Legislature:

- Home telephone numbers, including cell phone numbers, should not be disclosed.
- Public agencies should notify individuals that their home addresses may be disclosed pursuant to OPRA requests.
- Individuals should be permitted to provide an address of record for disclosure purposes, in addition to their home address when interacting with public agencies.
- The Governor or Legislature should establish objective guidelines defining when and from which government records home addresses should be redacted.
- Individuals should be permitted to opt out of disclosure of their home addresses.
- In the future, computer systems and applications should be programmed to collect but not disclose home addresses and telephone numbers.

This report, including the policy recommendations contained therein, will be incorporated in the final report of the New Jersey Privacy Study Commission at the conclusion of its complete study of the privacy issues raised by the collection, processing, use and dissemination of information by public agencies.

The Special Directive to the Privacy Study Commission

This report responds to Executive Order 26, in which Governor McGreevey 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..."¹³

The Legislature created the New Jersey Privacy Study Commission in the Open Public Records Act 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."¹⁴

The Privacy Study Commission ("Commission") is a temporary body consisting of 13 members representing groups that advocate citizen privacy interests and groups that

¹³ Executive Order 26, dated August 13, 2002, may be found at the following website:
<http://www.state.nj.us/infobank/circular/eom26.shtml>.

¹⁴ N.J.S. 47:1A-15. The full text of the New Jersey Open Public Records Act may be found at
<http://www.state.nj.us/grc/act.html#privacy>.

advocate increased access to government records. Its membership includes representatives of local law enforcement agencies, one local government official, attorneys practicing in the fields of municipal law and individual privacy rights, representatives of educational professionals and organizations, one crime victim advocate, one representative of the news media, one legislative expert and one retired member of the state judiciary. The Special Directive Subcommittee is a subset of the Commission created to address the specific issue of whether and to what extent home addresses and home telephone numbers of citizens should be made publicly available to public agencies (the “special directive”).¹⁵

A. Recommendations

The New Jersey Open Public Records Act (“OPRA”) favors disclosure of public records. 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.”¹⁶ Any limitations on the right of access are to be construed in favor of the public’s right of access.

OPRA also specifically states that “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.”¹⁷ Thus, the right of privacy is secondary to the public right to access.

In establishing its recommendations regarding whether and to what extent home addresses and home telephone numbers, including cell phone numbers, should be made publicly available by public agencies, the Commission considered the legislative findings that favor disclosure while also protecting privacy.

The Commission 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. Home Telephone Numbers, Including Cell Phone Numbers, Should Not Be Disclosed

It is often difficult for records custodians to determine whether the home telephone numbers, including cell phone numbers, in government records are commercially listed

¹⁵ Members of the Special Directive Subcommittee are: Grayson Barber (Chair of the subcommittee), Thomas J. Cafferty, George Cevasco, Edith A. Fulton, Hon. Rosemary Karcher Reavey, J.S.C. (retired), William John Kearns, Jr., M. Larry Litwin (Chair of the Privacy Study Commission) and Karen Sutcliffe. Other members of the Privacy Study Commission are: Richard P. DeAngelis, Jr., John Hutchison, Pamela M. McCauley, Jack McEntee, and H. Lawrence Wilson, Jr. The Privacy Study Commission gratefully acknowledges the assistance of its staff attorney, Catherine Starghill, and the generous support of the New Jersey Department of Community Affairs in making Ms. Starghill available to the Commission.

¹⁶ N.J.S.A. 47:1A-1.

¹⁷ Id.

or unlisted by regional telephone companies. This means that for practical purposes, records custodians may not be able to comply with the provision of OPRA that directs them to redact unlisted telephone numbers from requested records.¹⁸ Therefore, the Commission recommends that all home telephone numbers, including cell phone numbers, not be disclosed under OPRA.

While this recommendation may be implemented for future records through the inclusion of a “check box” that requires individuals to identify whether the telephone number listed on all new government forms and applications is in fact a home telephone number, it is problematic for existing records. Thus, the Commission recommends that the Governor or Legislature mandate a divided approach for implementing this recommendation. As to records created prior to the inclusion of this “check box”, all telephone numbers in government records should not be disclosed pursuant to OPRA requests unless the record clearly identifies that the telephone number is not a home telephone number. This will not harm requestors since they may utilize other resources to obtain commercially listed home telephone numbers, including regional telephone directories or Internet search engines.

2. Public Agencies Should Notify Individuals that Their Home Addresses May Be Disclosed Pursuant to OPRA Requests

Many people are unaware that currently under OPRA their home address may be publicly disclosed when they give this information to public agencies. Several private citizens testified at the Commission’s open public hearings that when they give information about themselves to the government they expect it to go no further.

Accordingly, the Commission recommends that the Governor or Legislature require public agencies to provide notice that home addresses may be disclosed. This may be accomplished by mandating that all public agencies include a notice widely visible in the public areas of their offices and on all new government forms and applications that reads, “Your home address may be disclosed pursuant to an OPRA request.”

(This recommendation assumes that the Governor or Legislature adopts Recommendation 1. If that recommendation is not adopted and implemented, then the Commission recommends that public agencies should notify individuals that both home addresses and telephone numbers may be disclosed pursuant to OPRA requests.)

3. Individuals Should Be Permitted to Provide an Address of Record For Disclosure Purposes, In Addition to Their Home Address When Interacting with Public Agencies

In many cases, public agencies collect home addresses from individuals not for the purpose of establishing domicile or performing other statutorily required functions, but for other purposes such as future contact and correspondence. Therefore, the Commission

¹⁸ N.J.S.A. 47:1A-1.1.

recommends that individuals who do not want their home addresses to be disclosed under OPRA should, when appropriate, have the option of also providing an address of record for disclosure purposes when public agencies respond to OPRA requests.

The Commission recommends that the Legislature implement this recommendation by mandating that all new government forms and applications request both an actual home address and an address of record. Public agencies will then have the actual home address to perform their legislatively mandated functions as necessary, but will only disclose the address of record (if one is provided) pursuant to OPRA requests. Actual home addresses should remain accessible to law enforcement, public safety and in real estate records necessary for land transactions, title searches, and property tax assessments.

4. The Governor or Legislature Should Establish Objective Guidelines Defining When and From Which Government Records Home Addresses Should Be Redacted

It is commonly understood that many records have been in the public domain as a matter of course ever since records have been collected and maintained by public agencies, such as real estate records necessary for land transactions, title searches and property tax assessments. Public agencies should continue to disclose these records to facilitate the execution of land transactions or in the fulfillment of statutorily required functions (as is the case for tax assessments). In other cases, however, the functions of public agencies do not strictly rely on the disclosure of home addresses and individuals providing agencies with this information may not expect that the agencies will disclose their information.

Since OPRA does not permit records custodians to ask requestors their reasons for requesting government records to determine whether the disclosure of the home addresses would violate an individual's reasonable expectation of privacy, records custodians need objective guidelines that define when and from which government records home addresses should be disclosed under OPRA. The Commission has identified two strategies for developing such guidelines:

a) Identify Categories of Records From Which Home Addresses Should Be Redacted

In addition to those records currently exempt from disclosure under OPRA, the Commission recommends that the Governor or Legislature identify those government records from which home addresses should not be redacted and those records from which home addresses should be redacted in the interest of safeguarding an individual's reasonable expectation of privacy. This exercise would be an enhancement to OPRA and may result in an amendment to the statute. The Commission further recommends that the Governor or Legislature garner the assistance of the Department of the State - Division of Archives and Records Management ("DARM") to execute this recommendation.

DARM's Implementation of this Recommendation

Existing DARM infrastructure may expedite the execution of this recommendation. Specifically, DARM has compiled a comprehensive list of all the records created, filed and maintained by every public agency in the State of New Jersey, along with retention schedules and other record keeping requirements established and approved by the State Records Committee. This compilation of retention schedules could become the basis for a *register* of all records of public agencies that is expanded to include detailed information on each record indicating whether the record contains home addresses that should be redacted.

DARM offered this proposed “register” for consideration and inclusion in OPRA as a keystone for the implementation of the intent of the act and had sought to secure funding for new software necessary to create it. The Commission recommends the implementation of this register as a practical and comprehensive means of establishing objective guidelines defining when and from which records home addresses should be redacted.

This recommendation is a practical approach for providing guidance to records custodians because custodians are already familiar with DARM’s records retention schedules and use them often in their daily operations. Therefore, the Commission believes that records custodians may easily incorporate in their daily operations review of an expanded compilation of records retention schedules that include detailed information on each record regarding whether home addresses contained therein should be redacted when processing OPRA requests.

The Commission also recommends that the funding for the creation and maintenance of the register, which will require research to determine the privacy requirements of each record and new software to create the register, come from DARM’s portion of the newly established New Jersey Public Records Preservation Account. The Public Records Preservation Account was created for the management, storage and preservation of public records from the monies received by county clerks attributable solely to the amount of increases to the document filing fees established by the Legislature in July 2003.¹⁹

The Commission further recommends that DARM consider several factors to determine whether home addresses should be exempted.²⁰

- The type of record;
- 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,

¹⁹ N.J.S.A. 22A:4-4.2.

²⁰ These factors are enumerated in United States v. Westinghouse Electric Corp., 638 F.2d 570 (3d Cir. 1980).

- Whether there is an express statutory mandate, articulated public policy or other recognizable interest militating toward access.

In conducting its study, the Commission implores DARM to devote special attention to an individual's reasonable expectation of privacy in records of vital statistics, professional licensing records, and recreational licensing records just to name a few.²¹

b) Identify Groups of Individuals Whose Home Addresses Should Be Redacted

In addition to identifying categories of records from which home addresses should be redacted, the Governor or Legislature should exempt certain groups of individuals from the disclosure of their home address due to the demonstrable safety risks to the members of these groups.²²

The Commission recommends that the home addresses of the following groups of individuals be redacted unless disclosure is required by any other statute, resolution of either or both Houses of the Legislature, regulation promulgated under the authority of any statute or Executive Order of the Governor, Executive Order of the Governor, rules of court, any federal law, federal regulation or federal order:

1. Active and former law enforcement personnel, including correctional and probation officers;
2. Judges;
3. Current and former attorneys general, deputy and assistant attorneys general, county and municipal prosecutors, and assistant county and municipal prosecutors;
4. Crime victims;
5. Personnel of the department of human services - division of youth and family services whose duties include the investigation of abuse, neglect, exploitation, fraud, theft, and other criminal activities;
6. Personnel of the department of treasury – division of taxation or local government whose responsibilities include revenue collection and enforcement; and,
7. Current and former code enforcement officers.

²¹ 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, and scores of other pieces of information. These records contain personal information including a person's physical description (age, photograph, height, weight, and eye color); race, nationality, and gender; family life (children, marital history, divorces, and even intimate details about one's marital relationship); residence, and contact information (address, telephone number, value and type of property owned, and description of one's home); political activity (political party affiliation, contributions to political groups, and frequency of voting); financial condition (bankruptcies, financial information, salary, and debts); employment (place of employment, job position; salary, and sick leave); criminal history (arrests, convictions, and traffic citations); health and medical condition (doctor's reports, psychiatrist's notes, drug prescriptions, diseases and other disorders); and identifying information (mother's maiden name, and Social Security number).

²² For example, judges and law enforcement officers may be targets of retaliation and crime victims may be targets of further intimidation and harassment.

There may be other groups of individuals whose positions create a demonstrable safety risk not set forth in this list. If that is so, the Commission believes it would be appropriate to similarly exempt such other groups of individuals by legislative regulation or Executive Order.

Members of the Commission have expressed concern over the practical difficulties associated with implementing this recommendation. Specifically, it is believed that there may be difficulties identifying whether an individual whose home address is listed in government records are members of an exempt group. However, it is also believed that this may be resolved in the future by mandating that all individuals completing government forms and applications requiring home addresses indicate whether they are members of any of the exempt groups. This may be accomplished by also mandating that all new government forms and applications that request home addresses have “check boxes” for the identification of an individual as a member of an exempt group. With regard to existing records, those entitled to this privacy protection will have an affirmative obligation to notify public agencies of their protective status.

Several members of the Commission believe that no group of individuals should be given special treatment regarding the nondisclosure of their home addresses as is provided in this recommendation.

5. Individuals Should Be Permitted To Opt Out of Disclosure of Their Home Addresses

This recommendation is offered as an alternative to Recommendation 3. discussed above. The Commission believes it may be appropriate in some cases to give individuals a means to indicate that they do not want their home addresses disclosed to the public under OPRA. Therefore, the Commission recommends that a study be conducted to determine which government forms and applications requiring home addresses are appropriate for the opt out option due to the potential for abuse (e.g. selecting such an option to avoid law enforcement). It is believed that this study may be conducted by DARM in conjunction with the Commission’s recommendation 4.a. discussed above.

After determining which government forms and applications are appropriate for the opt out option, the Governor or Legislature may mandate that this option be implemented by including an “opt out” check box on all new government forms and applications in the future.

One member of the Commission specifically disagrees with this recommendation, opining that, in light of the other recommendations in this report, there is no need for this provision and further opining that this provision could lead to an incomplete public record.

6. In the Future, Public Agencies Should Program Their Computer Systems and Applications to Collect But Not Disclose Home Addresses and Telephone Numbers When Redaction is Required

In the future most OPRA requests will likely be answered in electronic form, making computer systems and application design a technological answer to ensuring that home addresses and home telephone numbers, including cell phone numbers, are not disclosed when redaction is required. Therefore, the Commission recommends that as new computer systems and applications are phased in, they should be designed to flag the data fields for home addresses and home telephone numbers, including cell phone numbers, and automatically redact this information when required by public agencies responding to OPRA requests. This recommendation does not pertain to existing government records in hardcopy or electronic form.

B. Public Comment

The Commission held seven public hearings on the issue of whether and to what extent individuals' home addresses and home telephone numbers should be made publicly available by public agencies. The hearings were held at locations in northern, southern and central New Jersey. The Commission received live testimony and written comments from individuals and organizations throughout the state. The following section is based upon live testimony and written comments (including e-mails) from the public received by the Commission through March 2004.²³

On the subject of home addresses in open public records, the views expressed 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 be disclosed.²⁴

1. Arguments Against Disclosing Home Addresses and Telephone Numbers Under OPRA

Academic Expert

Professor Daniel J. Solove, Associate Professor of Law at Seton Hall Law School in New Jersey, submitted written comments regarding his assertion 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.²⁵ 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 telephone numbers, citing 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). He also stated that the United States Court of Appeals for the Third Circuit 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," citing Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999).

Professor Solove also asserted that if New Jersey were to routinely give out home addresses and home telephone numbers, it may not only be violating the U.S.

²³ The Commission meets approximately once a month and invites the public to attend and comment on its work. This report incorporates public comments from these regular meetings, as well as from special public hearings. The regular monthly meetings are not taped, so written testimony is in the record but transcripts of those meetings are not available.

²⁴ Most of the comments received by the Commission deal only with home address information. The Commission assumes that the points of view and courses of reasoning apply to home telephone numbers, as well as to home addresses.

²⁵ Professor Solove recently published a legal text entitled, "Information Privacy Law" (Aspen Publishing, 2003) (with Marc Rotenberg), and has written extensively on the subject.

Constitution (as interpreted by many federal courts of appeal including, most importantly, the Third Circuit), but it may also be repudiating the privacy protections of the federal Freedom of Information Act approach, which is the approach on which most states' open public records acts are modeled.²⁶

Further, Professor Solove stated that “[t]his conclusion certainly doesn’t mean that New Jersey is barred from disclosing addresses and telephone numbers in public records. But it does mean that any such disclosures will be balanced against the state’s interest in disclosing them. . . . It is important to note that the personal information in public records is often compelled by the government. People don’t give it out freely but are often forced to do so. Broad disclosure of people’s addresses can compromise people’s safety. It may benefit the media, which wants easy access to information, and commercial interests, which want to use addresses for marketing purposes. But in balancing under the Constitution, courts look to the extent to which the greater public interest is served by disclosure.”

New Jersey Department of Human Services

The New Jersey Department of Human Services (DHS) provided a “statement of concern” in which the DHS Office of Education noted that it does not believe that the Internet is a secure medium for maintaining government records that often contain personal information.

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 stated that there should be a presumption that such information remains 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.²⁷ The ACLU-NJ proposed that two exceptions should apply to the confidentiality of home addresses: voter registration records and tax assessment records. They stated that these records containing home addresses should be disclosed, whereas all other records containing home addresses should remain confidential. As to financial records, the

²⁶ 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).

²⁷ 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 since they are individually addressed at the federal level via the Financial Services Modernization Act and the Health Insurance Portability and Accounting Act, respectively.

ACLU-NJ recommended one exception for the disclosure of the salaries of public employees.

The ACLU-NJ stated that citizens disclose their home addresses because they are compelled to do so by state law and in order to receive basic governmental services. According to the ACLU-NJ, citizens 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 citing the following Meghan's Law cases: Doe v. Poritz, 142 N.J. 1 (1995); Paul P. v. Farmer, 227 F.3d 98, 101 (3d Cir. 2000); and Paul P. v. Verniero, 170 F.3d 396 (3d Cir. 1999).

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.

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 personal 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.

New Jersey Education Association

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 Association's representative testified that "NJEA believes in accessible and transparent government. However, we believe that in the pursuit of that ideal it is important that government not allow the privacy rights of individuals to be trampled. ... We are particularly concerned about the potential impact of releasing information about school employees as a distinct class."

New Jersey School Boards Association

The New Jersey School Boards Association, a non-partisan federation representing elected officials of more than 600 school districts, stated that the Legislature should exempt from disclosure the home addresses and telephone numbers of school board members. "To promote community participation and encourage a broad pool of candidates for school board elections, the government should not require school board members to give up their reasonable expectation of privacy simply because they want to serve their community." The Association's representative further recommended that "the

home addresses and home telephone numbers of citizens should never be disclosed by public agencies unless such disclosure is required by law enforcement agencies.”

New Jersey Principals and Supervisors Association

In written testimony, the New Jersey Principals and Supervisors Association stated that “if the home addresses and telephone numbers of school administrators are easily released to the public, there is the potential for harassment of these leaders and even abuse. Our past experience indicates that such incidents do occur.”

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.”

Municipal Clerk of the Borough of Paramus

One submission, from the Municipal 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 chairman 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

Dozens of 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.”²⁸ 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.

²⁸ 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.

Several witnesses stated that the government should disclose no personal information about them.

Complaining specifically about unsolicited junk mail from mortgage services companies, one witness stated that “even though I am in the financial services business myself, I have absolutely no sympathy for the companies who mine this personal information for their own ends. The complaints from realtors groups, mortgage services companies, and credit card companies should not outweigh the right of citizens to a little privacy -- especially when concerning financial information.”

Another witness complained specifically about receiving solicitations from attorneys who use motor vehicle accident reports to solicit prospective clients. One e-mail said, “I believe that the state government and state agencies are entirely too free with information that should not be public.” Another answered the question of whether and to what extent home addresses and home telephone numbers of citizens should be made publicly available by public agencies as “None and NEVER.”

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 and Telephone Numbers Under OPRA

Academic Expert

Professor Fred H. Cate, Professor at Indiana University School of Law-Bloomington, submitted written comments and testified before the Commission regarding his assertion that no constitutional privacy right attached to home addresses and home telephone numbers.²⁹ He stated that the constitution does not prohibit public access to home addresses and telephone numbers in government records. In fact, he stated that the Constitution permits and even encourages public access to such information. He further stated that assertions to the contrary are “incorrect as a matter of law.”

Professor Cate also stated that scholars and courts have identified many rights to privacy in the Constitution.³⁰ However, he further stated that while those rights are all important

²⁹ Professor Cate is a distinguished professor and director of the Center for Cybersecurity Research at Indiana University School of Law-Bloomington, IN. He has researched, taught and written about information privacy issues for 13 years.

³⁰ Professor Cate stated that the rights of privacy in the Constitution include the rights to be free from unreasonable searches and seizures by the government, to make decisions about contraception, abortion, and other “fundamental” issues such as marriage, procreation, child rearing, and education, the rights to disclose certain information to the government, to

rights, most of them have nothing to do with the government's disclosure of home addresses and telephone numbers in government records. According to him, few of those rights involve privacy of information at all.

Professor Cate stated that there is only one U.S. Supreme Court case that articulates a constitutional right in the nondisclosure of information, although it does so in the context of nondisclosure *to* the government, rather than any obligation of nondisclosure *by* the government, citing Whalen v. Roe, 429 U.S. 589. He further stated that the U.S. Supreme Court has never decided a case in which it found that disclosure *to or by* the government violated the constitutional right recognized in Whalen.

Professor Cate stated that there is no right to privacy guaranteed by the Constitution that would speak in any way to the government's disclosure of home addresses. For example, he stated that the United States Court of Appeals for the Fourth Circuit struck down the Drivers Privacy Protection Act, 18 U.S.C. §§2721-2725, stating that "neither the Supreme Court nor this Court has ever found a constitutional right to privacy with respect to the type of information found in motor vehicle records. Indeed, this is the very sort of information to which individuals do not have a reasonable expectation of privacy," citing Condon v. Reno, 155 F.3d 453, 464 (4th Cir. 1998); reversed on other grounds, Reno v. Condon, 528 U.S. 441 (2000).

Professor Cate further cited U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999), certiorari denied, 528 U.S. 1188 (2000), for the proposition that if government agencies decline to publish information, the agencies should have the burden to show that dissemination of the information would inflict *specific and significant harm* on individuals.

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. NJFOG emphasized the axiom that free speech, and by extension open public records, are essential for representative democracy. NJFOG stated that to ban the disclosure of home addresses would undermine OPRA and impair the ability of the news media to do investigative reporting. The organization's representative stated that 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 further stated 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 restrict disclosure and, within that minority, home addresses are protected only for discrete groups such as judges

associate free from government intrusion, and to enjoy one's own home free from intrusion by the government, sexually explicit mail or radio broadcasts, or other intrusions.

and law enforcement officers. NJFOG argued that the disclosure of home addresses is significantly less intrusive than the disclosure of Social Security Numbers, and further stated that most people do not seem to attach much value to the privacy of their home addresses since commercial telephone directories routinely publish this information.

NJFOG also stated that it believes that the redaction of home addresses from government records is a labor-intensive and costly proposition. NJFOG expressed concern that the burden of the expense might be imposed upon requestors of government records. The organization highlighted that 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.”

NJFOG recognized that “people, in certain circumstances, may have an interest in keeping their home address or telephone number private.” But it maintained that any suggestion that the federal or state constitution could protect this information would be “philosophically flawed, administratively impractical, unnecessarily sweeping and a serious threat to the goal of open government.”

New Jersey Press Association

The New Jersey Press Association stated, “there is no right of privacy protecting home addresses under the United States or New Jersey Constitution.”

Asbury Park Press

Two representatives of the Asbury Park Press testified on the value of home addresses to newspapers. They stated that journalists perform a critical “watchdog” function serving as the public’s eyes and ears to monitor the affairs of government. They further stated that losing access to home addresses could impair the newspaper’s ability to track sources and impede the function of newspapers in fulfilling their role that may be characterized as an essential part of the system of checks and balances on government.

The representatives also stated that the newspaper’s code of ethics requires that anonymous sources be corroborated and that this often requires checking public sources of information to ensure accuracy in reporting. They added that newspapers use home addresses as an extension of one’s name to further ensure accuracy in reporting.

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 comments suggesting that restrictions on the disclosure of home addresses would impair news reporting.

Commercial Resellers 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 the largest commercial reseller of government records (on a subscription basis) in the United States, urging the Commission not to exempt home addresses from disclosure under OPRA. They stated that the databases compiled from government 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.

Real Estate and Title Search Professionals

Several real estate and title search companies testified that they need government records containing home addresses for the purpose of facilitating real estate transactions. They further stated that in the current market, some real estate transactions require 24-hour turnaround. They asserted that the purchase and sale of real estate requires extensive review of government records that have traditionally been open for public inspection, such as property deeds, mortgages, municipal tax assessment records, tax liens and judgment liens. These witnesses urged the Commission not to restrict these government records now.

A California company, DataTrace, testified that it is building a database from real property records it obtains from New Jersey county clerks’ offices, as well as from tax and judgment records. They stated that the database will be made available on a subscription basis and is critical to its business.

A New Jersey company, Charles Jones, LLC, indexes judgments, liens and bankruptcies, and provides advanced database management services in support of real estate transactions throughout New Jersey and the Mid-Atlantic states. Its representative specifically asked the Commission not to conclude in its final report that there could be any constitutional protection for home addresses.

A company affiliated with Charles Jones, Superior Information Services, emphasized that information from public records can be used to feed the credit reporting system, which

underlies, in large measure, the economic systems of the nation. These companies urged the Commission to recommend no restrictions on the disclosure of home addresses.

Tax Collectors and Treasurers Association of New Jersey

A representative of the Tax Collectors and Treasurers Association of New Jersey, presented his organization's concerns regarding the need for public or limited disclosure of home addresses for tax sales, foreclosures and parties of interest to real estate transactions (such as taxpayers, real estate owners and heirs, prior tax lien holders, and occupants).

Association of Municipal Assessors of New Jersey

The Association of Municipal Assessors of New Jersey emphasized the need to ensure that local assessors have the ability to ascertain home addresses from certain government records, particularly recorded property deeds. "Assessors must have an appropriate address to identify properties as a means of ensuring the fair and equitable assessment of all properties under their jurisdiction."

New Jersey Land Title Association

A representative of the New Jersey Land Title Association addressed the Commission regarding the necessity of public or limited disclosure of home addresses for title searching and tax lien verification. He stated that title search companies use property addresses to determine whether there are judgments or liens against properties.

Geographic Information Systems Professional

The Commission also heard testimony from the coordinator of Geographic Information Systems in Somerset County. 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."

Professional Investigators

The Commission received verbal and written testimony from several professional investigators, who emphasized the value of government records, and home addresses in particular, for performing services related to law enforcement. They asserted that these services include 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 that they adhere to a voluntary code of professional conduct,³¹ and that their state licensing requires 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 government records or some other means.

Attorneys

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

Private Citizens and Other Comments

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 addresses 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. One letter received by the Commission expressed concern that unless home addresses were disclosed, real estate transactions would have to be processed manually which would take more time and manpower thus increasing the cost of the transactions. One individual pursued an avocation of testing the responsiveness of state agencies in responding to OPRA requests, and urged the Commission to resist, on principle, any limits on open government.

One individual urged the Commission to allow volunteer organizations the opportunity to receive names and addresses from local government. He stated that "without the access to [home addresses], volunteer organizations could not continue to serve their community. This is the primary source of income through mailings requesting donations to support the organization."

In written testimony, a landlord explained that a broad statewide rental assistance program has begun a process of requiring landlords to identify "comparable rents" when setting the rent for an assisted dwelling. In order to find such information, he stated that small landlords, in particular, require access to home addresses from government clerks.

³¹ The self-regulatory framework of Individual Reference Services Group (IRSG) is outlined in a report to Congress: www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.

C. Other Jurisdictions

All governments collect and use personal information in order to govern. Many of these records have long been open for public inspection. Democratic governments moderate the need for information with their obligation to be open to the people 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.

In an effort to protect the privacy of individuals, many jurisdictions in the United States have enacted specific legislation regarding the disclosure of home addresses and home telephone numbers. They are as follows:

- **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 of individuals: 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.

D. Legal Analysis

1. The New Jersey Open Public Records Act and Home Addresses

OPRA favors the disclosure of public records while acknowledging the state's "responsibility and obligation" to safeguard citizens' personal information. However, OPRA does not provide a definition of "personal information" or a "reasonable expectation of privacy." Nor does it contain a general exemption for home addresses and home telephone numbers. However, certain other personal information is exempted from disclosure under OPRA, including Social Security Numbers, credit card numbers, unlisted telephone numbers and drivers license numbers.³² The statute mandates that records custodians redact this information from government records disclosed pursuant to OPRA requests.³³

OPRA also provides an exemption for personal information that is protected from disclosure by other state or federal statutes, regulations, or executive orders.³⁴ For example, OPRA may not be used to obtain the residential home address of an individual who has obtained protection through the state's Address Confidentiality Program.³⁵

Conversely, OPRA specifically provides for the public disclosure of some home addresses, such as the residence of crime victims and criminal defendants listed in reports of criminal investigations.³⁶ However, this provision instructs records custodians to consider "the safety of the victim and the victim's family, and the integrity of any ongoing investigation" before disclosing such information.³⁷ 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."³⁸ Additionally, OPRA provides that no criminal convict should be granted access to information about the convict's victim, including the victim's home address.³⁹

The Commission observes an apparent contradiction regarding the accessibility of a crime victim's home address under OPRA. Although the statute provides that "a custodian shall not comply with an anonymous request for a government record which is protected under the provisions of this section,"⁴⁰ for practical purposes, records

³² N.J.S.A. 47:1A-1.1.

³³ N.J.S.A. 47:1A-5.

³⁴ N.J.S.A. 47:1A-9.

³⁵ 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.

³⁶ N.J.S.A. 47:1A-3(b).

³⁷ *Id.*

³⁸ *Id.*

³⁹ N.J.S.A. 47:1A-2.2.

⁴⁰ N.J.S.A. 47:1A-2.2(c).

custodians cannot determine whether the individuals identified in the records have ever been victims of crimes. Furthermore, records custodians cannot readily discern whether requestors are criminal convicts, especially in light of the fact that OPRA permits anonymous records requests. Therefore, it may be practically impossible to completely comply, at least in the case of anonymous requests, with OPRA. However, Recommendation 4.b. provides a resolution to this situation by identifying crime victims on all new government forms and applications, and not disclosing their home addresses pursuant to OPRA requests.

Thus, OPRA currently provides divergent treatment regarding the public disclosure of home addresses of individuals contained in government records.

2. Governor McGreevey's Executive Orders 21 and 26

The state's treatment of home addresses and home telephone numbers, including cell phone 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.⁴¹ The Order stated that "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 rescinded and replaced by Executive Order 26, which restored access to home addresses and publicly listed telephone numbers, but directed the Privacy Study Commission to analyze and report on this issue.⁴²

The Legislature (through OPRA) and Governor McGreevey (through Executive Orders 21 and 26) express concern over violating a citizen's reasonable expectation of privacy through the disclosure of personal information like home addresses and home telephone numbers, including cell phone numbers. However, both acknowledged the need for additional study and understanding of what a "citizen's reasonable expectation of privacy" means in the context of the potential disclosure of this information pursuant to OPRA requests for government records.

The Commission's recommendations were developed in light of the statutory and judicial interpretations of an individual's reasonable expectation of privacy in home addresses and home telephone numbers, including cell phone numbers, as well as policy considerations concerning the same.

⁴¹ Executive Order 21, dated July 8, 2002, may be found at the following website:
<http://www.state.nj.us/infobank/circular/eom21.shtml>.

⁴² Executive Order 26, dated August 13, 2002, may be found at the following website:
<http://www.state.nj.us/infobank/circular/eom26.shtml>.

3. Reasonable Expectation of Privacy in Home Addresses and Telephone Numbers

OPRA, in its legislative findings, declares “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.”⁴³ Because an individual’s “reasonable expectation of privacy” in home addresses is not explicitly defined in OPRA, the Commission turned to interpretations in federal statutes and judicial decisions for guidance.

a.) Statutory Interpretations of “Reasonable Expectation of Privacy” Regarding the Disclosure of Home Addresses

The federal government addresses the need for “open government” through its Freedom of Information Act (FOIA)⁴⁴ which generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions. Of those exemptions and special exclusions, one exemption is for “private matters” and another is for “other statutes,” including the Privacy Act (discussed below). Thus, although the goal of FOIA is full disclosure of government records, Congress concluded that some confidentiality is necessary.

FOIA is an information disclosure statute that, through its exemption structure, strives to strike a balance between information disclosure and nondisclosure, with an emphasis on the fullest responsible disclosure. Inasmuch as FOIA’s exemptions are discretionary, not mandatory,⁴⁵ agencies may make discretionary disclosures of exempt information, as a matter of their administrative discretion, where they are not otherwise prohibited from doing so.

Congress later enacted the Privacy Act to complement FOIA.⁴⁶ After extensive hearings and careful consideration of how best to protect privacy in an era of automated information systems, Congress passed the Privacy Act of 1974.⁴⁷ It is the most comprehensive privacy law in the United States.⁴⁸ The purpose of the Privacy Act is to balance the federal government’s need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy

⁴³ N.J.S.A. 47:1A-1.

⁴⁴ Freedom of Information Act (FOIA), 5 U.S.C. §552.

⁴⁵ See *Chrysler Corporation v. Brown*, 441 U.S. 281, 293 (1979); *Bartholdi Cable Co. v. FCC*, 114 F.3d 274, 282 (D.C. Cir. 1997) (FOIA’s exemptions simply permit, but do not require, an agency to withhold exempted information).

⁴⁶ Freedom of Information Act (FOIA), 5 U.S.C. § 552. The Privacy Act, 5 U.S.C. §552a, was adopted with amendments to FOIA in 1974.

⁴⁷ Privacy Act of 1974, 5 U.S.C. § 552a (1974).

⁴⁸ The United States Department of Justice has characterized the Privacy Act as a statute that is difficult to decipher and apply due to its imprecise language, limited legislative history, and somewhat outdated regulatory guidelines. U.S. Dept. of Justice, “Overview of the Privacy Act of 1974, May 2002 Edition” (last updated December 11, 2003).

stemming from federal agencies' collection, maintenance, use and disclosure of personal information.

The Privacy Act focuses on four basic policy objectives:

- (1) To restrict disclosure of personally identifiable records maintained by agencies.
- (2) To grant individuals increased rights of access to agency records maintained on them.
- (3) To grant individuals the right to seek amendment of agency records maintained on them upon a showing that the records are not accurate, relevant, timely or complete.
- (4) To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

The New Jersey Supreme Court has looked to FOIA and the Privacy Act for guidance in cases interpreting the "Right To Know Law"⁴⁹ and the Common Law Right to Know⁵⁰. 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). The Commission similarly looks to these statutes and the court decisions interpreting them for guidance in discerning the "reasonable expectation of privacy" articulated in OPRA.

As a starting point, we turn to the U.S. Supreme Court which has stated that individuals have a reasonable expectation of privacy with respect to their home addresses. Reading FOIA and the Privacy Act together, the Supreme Court explained this point in United States Dep't of Defense v. Fair Labor Relations Authority, 510 U.S. 487 (1994), as follows:

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

⁴⁹ 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."

⁵⁰ The alternative method to using OPRA to obtain non-public government records involves litigating for a right to access. A body of case law, historically known as the "Common Law Right to Know," generally provides broader access to government records, but requires a judicial balancing test. The balancing test requires that the documents are government records, the requestor have a good reason to inspect the records, and the requestor's reasons for inspecting the records outweigh the state's interest in confidentiality. See Irval Realty, Inc. v. Board of Public Utility Commissioners, 61 N.J. 366, 294 A.2d 425 (1972). 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.

are reluctant to disparage the privacy of the home, which is accorded special consideration in our Constitution, laws and traditions.” *Id.* at 501.

b) Judicial Interpretations of “Reasonable Expectation of Privacy” Regarding the Disclosure of Home Addresses

i. U.S. Supreme Court

The U.S. Supreme Court has not yet positively ruled on a constitutional right in the nondisclosure by the government of bare home addresses in government records. However, the court has recognized a constitutional right of privacy in the nondisclosure of certain personal information. Further, the court has only upheld that right, thus shedding light on what is meant by “a reasonable expectation of privacy in personal information” generally, in one instance.

In Whalen v. Roe, 429 U.S. 599 (1977), the court held that the constitutionally protected zone of privacy included the individual interest in avoiding disclosure of personal matters. *Id.* However, the court held that a state statute requiring that copies of prescriptions for certain drugs be provided to the state did not infringe on individuals’ interest in nondisclosure.

Similarly, in Nixon v. Administrator of General Services, 433 U.S. 425 (1977), the court held that President Nixon had a constitutional privacy interest in the personal records of his conversations with his family. However, the court also held that the challenged statute that allowed government archivists to take custody of the former President’s materials for screening did not impermissibly infringe on his privacy interests.

Conversely, the court has held that even a decedent’s family’s privacy interest outweighed public interest in disclosure of personal information and positively held for the nondisclosure of certain death-scene photographs of the decedent. See National Archives and Records Administration v. Favish, 124 S. Ct. 1570 (March 30, 2004).

ii. U.S. Court of Appeals for the Third Circuit

The U.S. Court of Appeals for the Third Circuit (the federal appeals court that governs New Jersey), unlike the U.S. Supreme Court, has specifically held in Megan’s Law cases that there are privacy interests in home addresses. In Paul P. v. Verniero, 170 F.3d 396, 404 (3d Cir. 1999), the court concluded that case law reflects the general understanding that home addresses are entitled to some privacy protection, whether or not so required by a statute. *Id.* at 404. The court also held that even sex offenders have a non-trivial privacy interest in their home addresses.⁵¹ *Id.* (quoting Dep’t of Defense at 501).

⁵¹ See also A.A. v. New Jersey, 341 F.3d 206 (3d Cir. 2003). In this Megan’s Law case, the court held that (1) sex offenders’ right of privacy in their home addresses gave way to the state’s compelling interest to prevent sex offenses, (2) the state’s internet publication of their home addresses did not violate offenders’ constitutional privacy rights, and (3) the

However, the court also held that Megan’s Law does not violate sex offenders’ constitutional right to privacy, either by requiring disclosure of home addresses⁵² or on the ground that required disclosures may place a strain on sex offenders’ family relationships⁵³.

This court also articulated the common law balancing test used to determine whether an individual’s privacy interest outweighs the public’s interest in disclosure in United States v. Westinghouse Electric Corp., 638 F.2d 570 (3d Cir. 1980). Specifically, the court stated that:

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 578.⁵⁴

While OPRA does not mandate this common law balancing test nor allow records custodians to inquire into the reason an individual has requested a particular government record, this analysis is instructive in an understanding of the meaning of a reasonable expectation of privacy regarding the disclosure of home addresses.

iii. New Jersey Supreme Court

The New Jersey Supreme Court has yet to rule on a case involving the public disclosure of bare home addresses in open government records. However, the court has addressed the public disclosure of an individual’s home address when coupled with other personally identifiable information in the Megan’s Law case of Doe v. Poritz, 142 N.J. 1, 84 (1995). The court’s ruling and reasoning provides guidance into an understanding of an individual’s reasonable expectation of privacy regarding the disclosure of home addresses.

In Doe, convicted sex offenders sought to enjoin enforcement of sex offender registration and community notification statutes (Megan’s Law). The court held that public disclosure of sex offenders’ home addresses, together with other information disclosed, *implicated a privacy interest* even if all the disclosed information may have been separately available to the public from other sources.

state’s compilation of information on them, including offenders’ names, ages, race, birth date, height, weight, and hair color, did not violate offenders’ constitutional right to privacy.

⁵² Id.

⁵³ Id. at 405

⁵⁴ These factors are included in Recommendation 4.a. “Identify Categories of Records From Which Home Addresses Should and Should Not Be Disclosed.”

However, the court highlighted the distinction between merely providing access to information and compiling and disclosing that information. In particular, the court stated that it believed a privacy interest is implicated when the government assembles those diverse pieces of information – name, appearance, address, and crime – into a single package and disseminates that package to the public, thereby ensuring that a person cannot assume anonymity (as was required under the community notification law). Id.

[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.

In the end, the court held that the state’s interest in public disclosure of sex offenders’ registration substantially outweighed the offenders’ privacy interest. Nevertheless, it is significant to the Commission’s study of the issue that the court recognized a privacy interest in home addresses when that information is disclosed with other personally identifiable information “ensuring that a personal cannot assume anonymity.”

c) Reasonable Expectation of Privacy in Home Addresses Versus Non-Governmental Disclosure of Home Addresses

Some members of the public have objected to the nondisclosure of home addresses by government agencies due to the fact that this same information may be obtained from non-governmental sources. Therefore, those who support this position argue that an individual whose home address and home telephone number are publicly published cannot reasonably expect any privacy in such information.

Supporters of this position further hold that if a piece of information can be found anywhere in the public domain, it should also be readily available from the state through OPRA. For example, they argue that if a citizen’s home address can be found in a commercial telephone directory, voter registration records, or property tax records, then there is no “reasonable expectation of privacy” in that information, and therefore the state should disclose the home address when it appears as part of any government record requested pursuant to OPRA.

Others assert that any inquiry on an online search engine (such as www.google.com) of a telephone number may provide a street address corresponding to the telephone number, and possibly even a map for locating the residence. Thus, the view holds that (at least for individuals with publicly listed their telephone numbers) there is no reasonable expectation of privacy in home addresses and home telephone numbers and so the state need not shield the same information from disclosure in government records.

Some individuals do not care if their addresses are published or disclosed by the government. However, for others it can be a matter of life or death. A vivid example of

this is the murder of Rebecca Shaffer, who was killed by a stalker who obtained her address from motor vehicle records.⁵⁵

Others, who object to government's disclosure of home addresses, believe that such disclosure is not justified by the fact that some - or even most - people allow their home addresses and home telephone numbers to be published by non-governmental sources. As the Third Circuit explained:

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."

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).

Moreover, those who oppose disclosure believe that just because a piece of information is in a "public record" doesn't mean it can be published for any purpose. Likewise, 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), that 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.

⁵⁵ This murder prompted Congress to adopt the Drivers Privacy Protection Act, 18 U.S.C. §§2721-2725, which regulates the disclosure of personal information contained in the records of state motor vehicle departments. See Reno v. Condon, 528 U.S. 441 (2000).

d) Standard for Recognizing a Reasonable Expectation of Privacy in Home Addresses

A question that has divided the courts and the members of the Commission is the standard for recognizing a “reasonable expectation of privacy.” One member of the Commission, for example, proposed recommending the creation of categories of individuals whose home addresses and telephone numbers would be exempt from disclosure, or alternatively recommended that records custodians be directed to deny access when there is “clear evidence of the substantial likelihood of harm or threat resulting from the disclosure of personal information.”⁵⁶

Another member, by contrast, stated that, as a municipal clerk, he believed members of the public had a reasonable expectation of privacy when they gave their personal information to his office. He agreed there should be categories of records that are accessible and non-accessible, but did not agree with the suggestion that the safety of a particular group of individuals by virtue of the nature of their employment (i.e., judges and law enforcement officers) was any more important than that of another group.⁵⁷

There is a split among the circuits on this issue as well. The U.S. Court of Appeals for the Tenth Circuit held that “the government must show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals...” in U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 528 U.S. 1188 (2000). The District of Columbia Circuit came out the other way on a very similar issue, holding that the government may restrict disclosure of people’s names and addresses in spite of a corporation’s First Amendment claim of entitlement to the information. Trans Union Corporation v. FCC, 245 F.3d 809, petition for rehearing denied, 267 F.3d 1138 (D.C. Cir. 2001).

Even under a “clear evidence of substantial likelihood of harm” standard, home addresses have a constitutional dimension. In Kallstrom v. City of Columbus, 136 F.3d 1055 (6th Cir. 1998), for example, the defense attorney for some drug dealers sought names and addresses from the personnel files of the police officers involved in the arrests. The court held that release of the information invaded the police officers’ privacy because it exposed them to a substantial risk of harm. Not only did it implicate their fundamental interest in personal safety, it violated constitutional rights. “The City’s release of private information ... rises to constitutional dimensions by threatening the personal security and bodily integrity of the officers and their family members.” Id. at 1064. The information extended beyond addresses, but the court’s reasoning suggests that the primary concern giving rise to the privacy interest was the officers’ safety, and it is the address information that is central to this safety concern.

⁵⁶ See New Jersey Privacy Study Commission meeting minutes of September 19, 2003 at http://www.nj.gov/privacy/minutes_091903.html.

⁵⁷ See New Jersey Privacy Study Commission meeting minutes of September 19, 2003 at http://www.nj.gov/privacy/minutes_091903.html.

E. Conclusion

The Commission believes that in some cases disclosure under OPRA of personally identifiable information such as home addresses may violate a citizen's reasonable expectation of privacy.⁵⁸ 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 Legislature has specifically articulated in OPRA its intention of not forcing individuals to sacrifice their privacy as a condition of doing business with the government when it stated that "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."⁵⁹ Likewise, Governor McGreevey articulated the same intention in Executive Orders 21 and 26.

The Commission believes an individual's reasonable expectation of privacy in his or her home address and telephone number may be violated in certain circumstances when the government discloses this information to the public. The potential for violating this reasonable expectation 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 used to involve 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.

In accordance with its mandate from Governor McGreevey, the Commission developed the following recommendations for consideration by the Governor and the Legislature:

- Home telephone numbers, including cell phone numbers, should not be disclosed.
- Public agencies should notify individuals that their home addresses may be disclosed pursuant to OPRA request.
- Individuals should be permitted to provide an "address of record" for disclosure purposes, in addition to their home address when interacting with public agencies.

⁵⁸ 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).

⁵⁹ N.J.S.A. 47:1A-1.

- The Governor or Legislature should establish objective guidelines defining when and from which government records home addresses should be redacted.
- Individuals should be permitted to opt out of disclosure of their home addresses.
- In the future, computer systems and applications should be programmed to collect but not disclose home addresses and telephone numbers.

The recommendations outlined in this report are based upon statutory and judicial interpretations of an individual's reasonable expectation of privacy regarding the disclosure by government of his or her home address and telephone number, as well as policy considerations of the same.

SECTION 3: REPORT ON COMMERCIAL USE

EXECUTIVE SUMMARY

As computerization and online availability of government records has made access easier a market has arisen for the secondary use of those records, i.e. use by businesses and entities other than the government. This secondary use has given rise to a tension between these businesses and entities and a citizen's interest in privacy. The Legislature has addressed privacy concerns through exemptions in OPRA and other statutes, such as worker's compensation and insurance laws. It has also left the door open for other exemptions through regulations, further legislation and executive order of the Governor.

The commercial use of government records, developed at the expense of the taxpayers, has created cost recovery issues separate and apart from the privacy concerns.

The use of government records by private businesses serves some important public purposes. It permits businesses to confirm credit history and property transactions, it permits investigators to detect insurance fraud and businesses to locate debtors. Further, it provides a data base for researchers, political parties and charities. There is concern, however, that some businesses may use government records for purely commercial benefit to themselves, at taxpayer expense and without any corresponding benefit to society. On the one hand, uses such as data mining or consumer profiling are perceived by some as abuses of access. On the other hand, the information sold by these secondary users (who are taxpayers as well) is often of assistance to local businesses, aiding their search for customers and clients and therefore playing a positive role in the economy.

Under OPRA (and the Right to Know Law preceding OPRA), a custodian may not question why the person requesting access wants the information. It is only upon a request for access to information under the common law right, where a balancing of the right of access against the need for confidentiality is required, that the reason for the request becomes relevant. Thus, in handling request for records under OPRA, if a distinction were made between those who seek the record for their own personal use and those who intend to make a secondary commercial use of the information, the custodian of the record would be required to inquire as to the use to be made of the information for each request. This would eliminate the distinction between the right of access under OPRA and the right of access under the common law. Since OPRA specifically retains the right of access under the common law it is clear the Legislature intended that the

statutory right and the common law right remain separate and the custodian may not inquire into the use of the records under OPRA.

There are those who argue that such an inquiry is ultimately beneficial if the government is permitted to impose a user fee of some sort upon the commercial user. Other states have declined to impose such a fee noting that statutory access is a right and not a revenue generating mechanism. The New Jersey courts have stated that the issue is for the Legislature to address.

The Legislature took the opportunity to review the right to access and the fees for access in OPRA and declined to make a distinction between private requestors and commercial requestors. The issue of commercial user fees is, therefore, outside the jurisdiction of the Privacy Study Commission.

FINDINGS

In 2002, the Legislature adopted the Open Public Records Act (“OPRA”), N.J.S.A. 47:1A-1 et seq. In that legislation, the Legislature created the New Jersey Privacy Study Commission 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.”

OPRA favors disclosure of public records. The preamble to the Act proclaims 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.”

In fulfilling its mission under OPRA, the Privacy Study Commission has created a series of subcommittees to address the issues raised by the collection, processing, use and dissemination of information by public agencies.” One of the subcommittees is the Commercial Use Subcommittee.⁶⁰

As noted in the Report of the Special Directive Subcommittee, states, including New Jersey, maintain records spanning an individual’s life from birth to death, including records of births, marriages, divorces, professional licenses, voting information, worker’s compensation information, personnel files (for public employees), property ownership, arrests, victims of crimes, criminal and civil court proceedings and scores of other pieces of information. These records, in turn, often contain personal information, including a person’s physical description, race, nationality, and gender; family life (children, marital history, divorces); residence, location, and contact information; political activity (political party affiliation, contributions to political group, frequency of voting); financial condition (bankruptcies, financial information, salary, debts); employment (place of employment, job position, salary, sick leave). While in New Jersey some of this information is rendered non-accessible by exemptions contained in OPRA or in Executive Orders or Regulations, nonetheless some of it remains publicly accessible. The accessibility of this personally identifiable information, in turn, creates a tension between concerns for individual privacy and the policy of transparency in government and the benefits flowing from such transparency.

The benefits that flow from open public records include:

- (1) Integrity of governmental operations and the political process. Specifically, open access to government records provides citizens with information necessary for critiquing government operations, evaluating the effectiveness and efficiency of government agencies, protecting against secret or illicit government activities, and

⁶⁰ William Kearns, Pamela McCauley, Grayson Barber, Catherine Starghill, Karen L. Sutcliffe and Thomas J. Cafferty constitute the members of the Commercial Use Subcommittee.

electing and monitoring public officials. This public benefit of open access to government records was perhaps best articulated by James Madison:

“Knowledge will forever govern ignorance. And people who mean to be their own Governors, must arm themselves with the power which knowledge gives.”⁶¹

- (2) Economic Benefits. Testimony adduced before the Commission makes clear that public access to government records permits commercial enterprises to accurately and efficiently identify consumers who may be interested in a given product or service, facilitates the ability to appropriately, expeditiously and economically grant credit to prospective borrowers, allows commercial entities to verify information in order to conduct business in a responsible manner, including complying with government regulations such as verifying driver’s license history for public transportation employment.
- (3) Law enforcement function. In 1998, the FBI alone made more than 53,000 inquiries to commercial online data bases.⁶² This was corroborated by testimony received by this Commission from a representative of Reed-Elsevier, a commercial subscription based retailer of information, who testified that their databases are often accessed by agencies engaged in compelling governmental interests such as identifying terrorists, apprehending criminal suspects, locating witnesses to crimes, and detecting insurance fraud.
- (4) Research. Clearly public records are used for studies concerning public health, traffic safety, the environment, crimes by all sorts of researchers, including journalists.

As is evident from the foregoing, a regime of access to public records serves a myriad of purposes ranging from acting as a check on government, fostering economic growth, protecting citizens against crime and apprehending criminals, to assisting research. Benefits are derived from a system of public access to government records not solely from the primary purpose of government in collecting, creating and maintaining the records but also from the secondary or derivative use of those records. Secondary or derivative uses of public records have been defined as “uses for purposes other than the official purposes for which the information was originally compiled.”⁶³ Examples of secondary or derivative uses of public records such as a labor union seeking a list of names, addresses, and phone numbers for federal employees so that it can contact employees for collective bargaining purposes. Similarly, a business seeking income data gathered as part of the U.S. Census in order to identify and target individuals for direct-

⁶¹ Writings of James Madison 103 (G. Hunt ed,1910).

⁶² Statement of Louis Freeh, former Director of the Federal Bureau of Investigation, before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and related Agencies, March 24, 1999.

⁶³ Privacy Rights v. FOIA the Disclosure Policy: The “Uses and Effects” Double Standard in Access to Personally-Identifiable Information and Government Records, 12 William & Mary Bill Rights.J.1 2003.

mail advertising for products ranging from burglar alarm systems for inner-city residents to luxurious ocean cruises for upscale suburban dwellers. Other examples of derivative uses of public records include use by journalists to investigate stories, use by corporate intelligence firms to conduct individual background checks and use by political and other organizations of names and addresses contained in public records to solicit new members or disseminate literature.⁶⁴

Tension may then arise between these secondary or derivative uses of public records with an interest in privacy of personally identifiable information contained in those records. Government records are the source of a considerable amount of personal information. Secondary or derivative users of personal information in government records include entities such as database resellers of information, direct marketing organizations, retail organizations, charitable and other non-profit organizations, and quasi-governmental and political organizations.

Many government records, particularly electronic records, have commercial value. Geographic Information Systems (GIS), a computer software program that links geographic information with descriptive information and can present layers of information with each layer representing a theme or feature of a map all of which then can be laid on top of one another creating a stack of information about the same geographic area. The systems are developed at considerable expense by the governmental entity and have clear commercial value to a private entity such as an engineering firm. Therefore, some government records, because of a commercial value derived from a particular secondary or derivative use, also implicate cost recovery issues separate from privacy issues.

These, then, are the issues to be addressed by the Commercial Use Subcommittee in this Report:

- (1) The implications of secondary or derivative use of personally-identifiable information contained in a government record; and,
- (2) The implications of commercial value in government records derived from a secondary use of that record, and the ability to recover that value.

⁶⁴ 12 William & Mary Bill of Rights Journal, p.1-2.

PUBLIC COMMENTS AND THE CURRENT LEGAL LANDSCAPE.

A. Public Comments

Some members of the public expressed their opposition to or support for the secondary or derivative commercial use of government records through personal testimony at the public hearings and open public meetings of the Commission, as well as written comments submitted to the Commission. The comments received by the Commission regarding the commercial use of government records are briefly summarized below.

Private Citizens

Several private citizens provided comments on the issue of commercial use of government records through the Commission's e-mail comment form. One citizen strongly urged the Commission to allow volunteer organizations to garner names and addresses from government records to solicit individuals through mailings for donations that he described as often being the primary source of income for such organizations. Other citizens, however, referred to attorneys' use of government records to identify potential motor vehicle accident and traffic violating clients as an "abuse of OPRA." Specifically, one citizen stated that, "OPRA should not be a tool used to enrich attorneys." Another citizen expressed concern with being "regularly inundated by unsolicited junk mail from mortgage services companies that have very private information" about his mortgage. He further stated that he had no sympathy for the companies that "mine this personal information for their own ends." He insisted that the complaints received by the Commission from realty groups, mortgage services companies, and credit card companies should not outweigh the right of citizens to a little privacy. He urged the Commission to take steps to stop this abuse of citizens' personal information.

Database Resellers of Information from Government Records

The Commission received testimony from a representative of Reed-Elsevier, the largest commercial subscription based retailer of information from government records in the United States. Their representative presented a plea for continued access to open government records so that they may create and maintain databases of the information contained therein for sale to their customers, who, Reed Elsevier claims are often engaged in compelling government interests such as identifying terrorists, apprehending criminal suspects, locating witnesses to crimes, and detecting insurance fraud.

Testimony was also received from the Direct Marketing Association (DMA), the oldest and largest trade association for businesses interested in direct marketing and database marketing. It has over 4,500 member companies in the United States and 53 other nations. The DMA's representative stated that commercial entities rely on open access to government records to help develop marketing campaigns and reach out to new

customers. She further stated that the ability to accurately and efficiently identify consumers who may be interested in a given product or service dramatically reduces costs, by eliminating undeliverable mail. She also stated that sending consumer offers and opportunities of interest to them enhances consumer satisfaction. She stressed the notion that new businesses that may not be able to afford mass market advertising, or that lack the customer lists of their well established competitors have the ability to reach potential customers and compete more effectively through their access to open government records.

The DMA claims to regulate its members regarding the personal privacy of consumers through the adoption by its Board of Directors of the “Privacy Promise.”⁶⁵ The Privacy Promise is a public assurance that all members of the DMA will follow certain specific practices to protect consumer privacy. Those practices are allegedly designed to have a major impact on those consumers who wish to receive fewer advertising solicitations while making compliance with the promise as easy as possible for DMA members.

Real Estate Professionals and Organizations

One company that describes itself as “fulfilling the vision of a standardized title and tax information system that spans the nation, enabling title insurance companies to streamline order processing and title production”⁶⁶ launched a letter writing campaign to the Commission by its employees expressing the concerns of the real estate industry regarding the real estate industry’s need for continued access to open government records. Specifically, DataTrace’s employees emphasized that if access to government records is denied or restricted, ordinary consumers may find it difficult and more costly to purchase or refinance a home because the title industry and mortgage institutions may have to engage in more manual processes for the verification of information that is now largely automated.

Charles Jones, LLC, a New Jersey based company whose mission is “to provide lawyers, lenders, title companies and abstracters with reliable information concerning judgments and other records filed in state and federal courts in New Jersey,” also weighed in with the Commission. This firm’s representative noted that professionals in real estate practice routinely rely on personal information in government records to determine property ownership and facilitate real estate transfers. He further stated that restricting access to personal information in government records would create more instances of mistakes and false identification, delay real estate closings, and increase the cost of real estate and financial transactions. He did, however, recognize that the definitions of public and non-confidential information should be carefully considered and that some safeguards may be required for certain information contained in government records.

⁶⁵ Adopted by the DMA Board of Directors in October 1997 and became effective as of July 1, 1999.

⁶⁶ DataTrace company website, company profile (September 30, 2003).

Professional Investigators

Individual professional investigators and the New Jersey Licensed Private Investigators Association (NJLPIA) presented verbal and written testimony before the Commission. These professional or private investigators testified that they are men and women who are “the protectors of private industry, corporations, business both small and large, individual citizens and attorneys seeking information in support of litigation or for the defense of the accused.” They claim that restricting their access to government records would “virtually wipe out an entire profession of persons whose lives are dedicated to helping others.” In the words of the President and Legislative Chair of NJLPIA, private investigators are “the first line of homeland security.”

They also stressed that, as a profession, they adhere to a voluntary code of professional conduct,⁶⁷ and that their state licensing requirements are very stringent and ensure that they are accountable for any misuse of personal information they obtain from government records.

Attorneys

Attorneys wrote to the Commission requesting that access to open government records not be restricted to members of their profession. The attorneys stated that they use government records (especially reports of motor vehicle accidents and traffic violations) as a resource for offering their services to prospective clients, locating witnesses and conducting investigations, a practice they insist is important to traffic violators, for example, because “many individuals are oblivious to what occurs to their driving record, insurance eligibility point assessment, auto insurance surcharges and the overall financial impact to them over several years as a result of a traffic offense.” One attorney indicated that 95% of his firm’s clients comes from the ability to obtain names and addresses from various municipal courts where complaints and summonses have been issued against traffic violators. Another attorney pointed out that the Canons of Ethics of the New Jersey Bar strictly regulate this process as a form of lawyer advertising in order to safeguard the public against any abuses emanating from it.

B. The Current Legal Landscape In New Jersey And Other Jurisdictions

Many states have legislatively addressed the increasing commercial value and/or use of government records⁶⁸, especially the commercial value of personal information contained in government records that may be used in ways that implicate a citizen’s privacy. Legislators have addressed this issue by enacting laws that attempt to balance longstanding policies of public access to government records with the privacy concerns of citizens. New Jersey legislators are currently balancing and further addressing the

⁶⁷ The self-regulatory framework of Individual Reference Services Group (IRSG) is outlined in a report to Congress: www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.

commercial value of personal information contained in government records with personal privacy protection through existing law and newly proposed law.

(1) Existing Law in New Jersey:

(a) Prohibition Against Commercial Use of Personal Information in Government Records.

New Jersey has one statute that prohibits the commercial use of government records.⁶⁹ This statute regulates the Department of Labor and it specifically applies to the Division of Workers Compensation. The statute limits the public's right to inspect and copy workers' compensation records for commercial use. Specifically, the statute provides that:

“... no records maintained by the Division of Workers' Compensation or the Compensation Rating and Inspection Bureau shall be disclosed by any person who seeks disclosure of the records *for the purpose of selling or furnishing for a consideration to others information from those records ...*”⁷⁰ (Emphasis added.)

The statute further provides⁷¹,

“... No information shall be disclosed from those records to any person not in the division, unless:

1. The information is provided in a manner which makes it *impossible to identify any claimant*;
2. The records are opened for the exclusive purpose ... to conduct an investigation ... in connection with any pending workers' compensation case ...;
3. The records are opened for the exclusive purpose ... to conduct an investigation ... in connection with the case, ... *and the party seeking access to the records certifies to the division that the information from the records will be used only for purposes directly related to the case*;
4. The records are subpoenaed...;
5. The division provides the information to another governmental agency pursuant to law, ... *which agency shall not subsequently disclose any of the information to [others] not entitled to receive the information*;
6. The information is information about the claimant requested by the claimant, ...” (Emphasis added.)

The constitutional validity of this statute withstood judiciary scrutiny when the New Jersey Supreme Court affirmed a lower court's decision that “[t]he Legislature could properly have found, in its enactment of this section relating to examination of

workmen's compensation records, without violating equal protection of the laws, a substantial good to be accomplished, that being the employment of the disabled, and an evil to be eliminated, that being commercial activities disclosing to employers for a profit the prior workmen's compensation histories of prospective employees with consequential non-hiring of victims of industrial accidents.⁷²

The Superior Court found that the statute satisfied substantive due process because the distinction between who may and who may not inspect and copy the records is not invidious to the point of denying commercial entities equal protection of the laws.⁷³ The court further found that the statute did not violate the right to freedom of speech because that right is not absolute and may be limited in order to obviate a threat to the public welfare.⁷⁴ Presumably, in this instance, the Legislature found a threat to the public welfare existed when it enacted this statute.

The Superior Court's decision in Accident Index Bureau, Inc. has, however, been discussed but never distinguished for the benefit of commercial entities seeking unencumbered access to inspect and copy other types of government records in several cases since 1967.⁷⁵

(b) Regulation of Commercial Use of Personal Information.

New Jersey also has one statute that regulates the commercial use of personal information – the Insurer Information Practices Act (IIPA).⁷⁶ Specifically, the Act establishes standards for the collection, use, and disclosure of information gathered by the insurance industry (as opposed to public agencies) in connection with policies, contracts or certificates of insurance for life, health, disability and property or casualty coverage.⁷⁷ IIPA applies to insurers, agents, insurance support organizations⁷⁸, and individuals requesting personal information in connection with an insurance transaction involving personal, family or household coverage.

The Act defines personal information as “any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about a person's character, habits, avocations, finances, occupation, general reputation,

⁷² Accident Index Bureau, Inc., 95 N.J.Super 39, 229 A.2d 812 (A.D. 1967), affirmed 51 N.J. 107, 237 A.2d 880, appeal dismissed 89 S.Ct. 872, 393 U.S. 530.

⁷³ Id. at 49.

⁷⁴ Id.

⁷⁵ See Oueilhe v. Lovell, 560 P.2d 1348, 93 Nev. 111, 115 (Nev. Mar 09, 1977), In re Look Magazine, 264 A.2d 95, 98, 109 N.J.Super. 548, 554 (N.J.Super.L. Mar 25, 1970), Ortley Beach Property Owners Ass'n v. Fire Com'rs of Dover Tp. Fire Dist. No. 1, 726 A.2d 1004, 1010, 320 N.J.Super. 132, 143 (N.J.Super.L. July 29, 1998), J.H. Renarde, Inc. v. Sims, 711 A.2d 410, 413, 312 N.J.Super. 195, 201 (N.J.Super.Ch. Feb 19, 1998), Sherman v. Sherman, 750 A.2d 229, 232, 330 N.J.Super. 638, 645 (N.J.Super.Ch. Jul 25, 1999).

⁷⁶ N.J.S.A. 17:23A-1.

⁷⁷ N.J.S.A. 17:23A-1(a) and (b).

⁷⁸ An “insurance support organization” collects or assembles information about individuals for the primary purpose of providing the information to an insurer or agent for insurance transactions. N.J.S.A. 17:23A-2(m).

credit, health or other personal characteristics.”⁷⁹ IIPA further defines privileged information as “individually identifiable information that relates to a claim for insurance benefits or a civil or criminal proceedings collected in connection with or in reasonable anticipation of a claim for insurance benefits or civil or criminal proceedings, and can include police investigation files as well as trade secret or other sensitive information.”⁸⁰

IIPA was based on the National Association of Insurance Commissioners’ Insurance Information and Privacy Protection Model Act.⁸¹ The New Jersey Department of Banking and Insurance has recognized that for the most part, IIPA provides more privacy protections than the Financial Services Modernization Act (“Gramm-Leach-Bliley”), 15 U.S.C. §6801 (1999).⁸² While the Gramm-Leach-Bliley privacy protections were enacted in 1999, New Jersey enacted its privacy protections some fourteen years earlier.

According to the sponsor’s statement, the objective of the IIPA bill when introduced before the New Jersey Senate was to balance the need for information by those conducting the business of insurance with the public’s need for “fairness in insurance information practices, including the protection of personal privacy and providing mechanisms by which natural persons and residents of this State may ascertain and dispute the accuracy of information gathered about them . . .”⁸³

In establishing a balance between insurers’ need for information and the public’s need for privacy, IIPA prohibits the disclosure of personal or privileged information about an individual without the written authorization of that individual, and then only if the disclosure of information is reasonably necessary to the “person” to perform a business, professional or insurance function for the disclosing institutions, agent or support organization and the person agrees not to make further disclosures.⁸⁴ Additionally, IIPA provides that any person who knowingly and willfully obtains information about an individual from an insurance institution, agent or insurance support organization under false pretenses is guilty of a crime in the fourth degree.⁸⁵

⁷⁹ N.J.S.A. 17:23A-2(t).

⁸⁰ N.J.S.A. 17:23A-2(w).

⁸¹ John P. Halvorsen, *Today’s Insurance Information Privacy: Why New Jersey Leads the Pack*, 211-Oct N.J. Law 39, 40 (2001).

⁸² *Id.* (Title V of the Financial Services Modernization Act protects the non-public personal information that individuals provide to financial institutions. These privacy requirements serve as the minimum standards states must enforce and permit states to enact consistent laws with stronger standards.)

⁸³ Senate, No. 1013—L.1985, c. 179.

⁸⁴ N.J.S.A. 17:23A-13.

⁸⁵ N.J.S.A. 17:23A-22.

(2) Proposed Legislation in New Jersey.

There is currently a bill before the New Jersey General Assembly that aims to exempt commercial requests for geographic information system maps from OPRA access.⁸⁶ This proposed amendment to OPRA⁸⁷ provides that,

“[s]ince the public’s access to government records is not intended for commercial gain, the custodian shall not permit a government record consisting of geographic information system (GIS) based mapping to be copied or otherwise provided for commercial use.”

The bill also provides for an amendment to OPRA records request forms that would include a certification that any government record requested that consists of GIS based mapping information will not be put to commercial use. Further, the bill would add a violation provision that provides,

“[a] person who knowingly files a request with a false certification that a government record consisting of GIS based mapping information will not be put to commercial use shall be guilty of a crime of the fourth degree and liable for a civil penalty, payable to the public agency, in an amount equal to twice the public agency’s cost to develop the GIS based mapping information. The Superior Court shall have jurisdiction of proceedings for the collection and enforcement of the penalty imposed by this section.”⁸⁸

(3) Other Jurisdictions.

The Legislatures in other states have addressed the issue of the commercial value of personal information in government records. These laws vary from state to state and range from strict prohibitions on the commercial use of government records to the establishment of cost recovery schemes. Some of the statutes exempt news reporting from the definition of commercial use, while others do not clearly define the commercial purposes they prohibit. The collage of states’ privacy protections from commercial use of personal information contained in government records may be summarized as follows:

Arizona - The Department of Health Services may promulgate rules and regulations as are required by state or federal law or regulation to protect confidential information and no name or other information of any applicant, claimant, recipient or employer shall be made available for any political, commercial or other unofficial purpose. A.R.S. §36-107.

⁸⁶ A2782, introduced May 10, 2004 and sponsored by Assemblymen Upendra J. Chivukula and Gordon M. Johnson.

⁸⁷ Proposed amendment to N.J.S.A. 47:1A-5(6)(d).

⁸⁸ Proposed amendment to N.J.S.A. 47:1A-12.

Another law dictates that voting precinct registers and other lists and information derived from registration forms (including name, party preference, date of registration, residence address, mailing address, zip code, telephone number, birth year, occupation, and primary and general election voting history) may be used only for purposes relating to a political or political party activity, a political campaign or an election, for revising election district boundaries and may not be used for a commercial purpose. A.R.S. §16-168.

The state's Public Records Act requires a person requesting copies, printouts or photographs of public records for a commercial purpose to provide a statement setting forth the commercial purpose for which the records will be used. The custodian of the records may then charge the requester a fee which includes: (1) a portion of the cost of the public body for obtaining the original or copies of the records, (2) a reasonable fee for the cost of time, materials, equipment and personnel required to reproduce the records, and (3) the value of the reproduction on the commercial market as best determined by the public body. A.R.S. §39-121.03(A). If the custodian determines that the commercial purpose stated is a misuse of the records, he or she may apply to the Governor to issue an executive order prohibiting the compliance with the records request. A.R.S. §39-121.03(B).

A person who obtains a public record for a commercial purpose without indicating that purpose or obtains a public record for a noncommercial purpose and uses or knowingly allows the use of the record for a commercial purpose or obtains a public record for a commercial purpose and uses or knowingly allows the use of the record for a different commercial purpose or obtains a public record from anyone other than a record's custodian and uses it for a commercial purpose shall be liable to the state or the public body from which the record was obtained for damages in the amount of three times the amount which would have been charge for the record had the commercial purpose been stated plus costs and reasonable attorney fees or three times the actual damages if it can be shown that the record would not have been provided had the commercial purpose of actual use been stated at the time of obtaining the record. A.R.S. §39-121.03(C).

For purposes of this statute, "commercial purpose" means the use of a public record for sale, resale or solicitation (not use as evidence, research for evidence in judicial or quasi-judicial action, or use for reporting by newspapers⁸⁹.) A.R.S. §39-121.03(D).

California - Under the state's Information Practices Act, an individual's name and address may not be distributed for commercial purposes, sold, or rented by an agency unless such action is specifically authorized by law. CA Civil §1798.60

Colorado - Records of official criminal actions and criminal justice records and the names, addresses, telephone numbers, and other information in such records may not be used for the purpose of soliciting business for pecuniary gain. The record's custodian may deny access to a record unless the requester signs a statement that affirms that the

⁸⁹ See Star Pub. Co. v. Parks, (App. Div.2 1993) 178 Ariz. 604, 875 P.2d 837, review denied.

record will not be used for the direct solicitation of business for pecuniary gain. C.R.S.A. §24-72-305.5.

Florida - Despite the Florida Sunshine Law's general exemption of social security numbers (SSNs) in government records, public agencies may not deny a commercial entity access to SSNs provided they will be used only in the normal course of business for legitimate business purposes (including verification of the accuracy of personal information received by a commercial entity in the normal course of its business; use in a civil, criminal, or administrative proceeding; use for insurance purposes; use in law enforcement and investigation of crimes; use in identifying and preventing fraud; use in matching, verifying, or retrieving information; and use in research activities). A legitimate business purpose does not include the display or bulk sale of SSNs to the general public or the distribution of such numbers to any customer that is not identifiable by the distributor. F.S.A. §119.0721(3).

As part of this law, the Florida Legislature acknowledged the fact that SSNs can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical and familial information, the release of which could cause great financial or personal harm to an individual and therefore intends to monitor the commercial use of SSNs held by state agencies in order to maintain a balanced public policy. F.S.A. §119.0721(7). Thus, the law requires that every agency file a report listing the identity of all commercial entities that have requested SSNs during the preceding calendar year and the specific purpose(s) stated regarding its need for SSNs. F.S.A. §119.0721(6).

Georgia - Under its insurance statutes, this state does not allow an employee of any law enforcement agency to allow any person, including an attorney, health care provider, or their agents, to examine or obtain a copy of any motor vehicle accident report or related investigative report when the employee knows or should reasonably know that the request for access is for commercial solicitation purposes. Likewise, no person may request any law enforcement agency to permit examination or to furnish a copy of any such report for commercial solicitation purposes. Ga. Code Ann., §33-24-53(c).

The law also prohibits a person from receiving compensation, a reward, or anything of value in return for providing names, addresses, telephone numbers, or other identifying information of victims involved in motor vehicle accidents to an attorney or health care provider which results in employment of the attorney or health care provider by the victims for purposes of a motor vehicle insurance claim or suit. Ga. Code Ann., §33-24-53(d). Any person who violates this law is guilty of a misdemeanor involving moral turpitude. Ga. Code Ann., §33.24-53(e).

Idaho - A claim for property tax relief and its accompanying documentation is not deemed to be public records and may not be used for an commercial purpose. ID ST §63-703.

Indiana - The state's Fair Information Practices requires any state agency maintaining a personal information system to refrain from preparing lists of the names and addresses of

individuals for commercial or charitable solicitation purposes except as authorized by law or by a rule promulgated by the oversight committee on public records. IC 4-1-6-2(i).

Another law provides that a state agency may adopt a rule and a political subdivision may enact an ordinance prescribing the conditions under which a person who receives information on disk or tape may or may not use the information for commercial purposes, including to sell, advertise, or solicit the purchase of merchandise, goods, or services, or sell, loan, give away, or otherwise deliver the information obtained by the request to any other person for these purposes. However, use of the information in connection with the preparation or publication of news, for nonprofit activities, or for academic research is not prohibited. A person who uses the information in a manner contrary to a rule or ordinance adopted under the law may be prohibited from obtaining copies or further data in the future. IC 5-14-3-3(e).

The law further prohibits the following lists of names and addresses from being disclosed by public agencies to commercial entities for commercial purposes and may not be used by commercial entities for commercial purposes:

- (1) A list of employees of a public agency;
- (2) A list of persons attending conferences or meetings at a state institution of higher education or of persons involved in programs or activities conducted or supervised by the state institution of higher education; and,
- (3) A list of students who are enrolled in a public school corporation if the governing body of the public school corporation adopts a policy prohibiting the disclosure of the list to commercial entities for commercial purposes or specifying the classes or categories of commercial entities to which the list may not be disclosed or by which the list may not be used for commercial purposes. IC 5-14-3-3(f).

Iowa - While the state provides that records of vital statistics are public records for certain purposes, the state registrar is allowed to refuse to permit these records to be used for purely commercial purposes. Op.Atty.Gen. (Pawlewski), March 29, 1974 (referencing I.C.A. §144.5).

Kansas - The state's Open Records Act provides that if access to public records or the purpose for which the records may be used is limited, an agency may require a person requesting the records to provide written certification that the requestor does not intend to, and will not (1) use any list of names or addresses contained in or derived from the records for the purpose of selling or offering for sale any property or service to any person listed or to any person who resides at any address listed or (2) sell, give or otherwise make available to any person any list of names or addresses contained in or derived from the records for the purpose of allowing that person to sell or offer for sale any property or service to any person listed or to any person who resides at any address listed. K.S.A. §45-220(c)(2).

Kentucky - A state law provides that a public agency from which copies of nonexempt records are requested for a commercial purpose may require a certified statement from the requestor stating the commercial purpose for which they will be used, and may require the requestor to enter into a contract with the agency. The contract will permit use of the public records for the stated commercial purpose for a specified fee which may be based on one or both of the following: (1) cost to the agency of media, mechanical processing, and staff required to produce a copy of the public record(s); and (2) cost to the agency of the creation, purchase, or other acquisition of the public records. KRS §61.874(4)(b) and (c). An agency also has discretion as to whether to provide access to public records in electronic form. If an agency does allow such access, it may require a commercial requestor to enter into a contract, license or other agreement, and may charge fees for these agreements not to exceed those elements of costs listed above. KRS §61.874(6).

This law also provides that it is unlawful for a person to obtain a copy of any part of a public record for:

- (1) a commercial purpose, without stating the commercial purpose, if a certified statement from the requestor was required; or
- (2) a commercial purpose, if the person uses or knowingly allows the use of the public record for a different commercial purpose; or
- (3) a noncommercial purpose, if the person uses or knowingly allows the use of the public record for a commercial purpose. A newspaper, periodical, radio or television station is not held to have used or knowingly allowed the use of the public record for a commercial purpose merely because of its publication or broadcast, unless it has also given its express permission for some other commercial use. KRS §61.874(5).

Missouri - The state's law prohibits the use for commercial purposes any information contained in any state or local voter registration system, limited to the master voter registration list or any other list generated from the information. Violation of this law is a class B misdemeanor. "Commercial purposes" means the use of a public record for the purpose of sale or resale or for the purpose of producing a document containing all or part of the copy, printout, or photograph for sale or the obtaining of names and addresses from public records for the purpose of solicitation or the sale of names and addresses to another for the purpose of solicitation or for any purpose in which the purchaser can reasonably anticipate the receipt of monetary gain from the direct or indirect use of the public record. V.A.M.S. 115.158(6).

Nebraska - The law provides that no sales or use taxes are imposed on the gross receipts from the sale, lease, or rental of and the storage, use or other consumption of copies of public records, except those documents developed, produced, or acquired and made available for commercial sale to the general public. Neb.Rev.St. §77-2704.42.

North Carolina - The public assistance recipient check register showing a complete list of all recipients of Work First Family Assistance in Standard Program Counties and State-County Special Assistance for Adults, their addresses, and the amounts of the

monthly grants are public records, but the registers or the information contained therein may not be used for any commercial or political purpose. Any violation of this law constitutes a class 1 misdemeanor. NC ST §108A-80.

South Carolina - The state's Family Privacy Protection Act of 2002 prohibits a person or private entity from knowingly obtaining or using any personal information obtained from a state agency for commercial solicitation. A person knowingly violating this law is guilty of a misdemeanor and, upon conviction, must be fined an amount not to exceed five hundred dollars or imprisoned for a term not to exceed one year, or both. South Carolina Code 1976 §30-2-50.

The state's Freedom of Information Act provides that a public body may, but is not required to, exempt from disclosure information of a personal nature where the public disclosure thereof would constitute an unreasonable invasion of personal privacy, including the name, address, and telephone number or other such information of an individual or individuals who are handicapped or disabled when the information is requested for person-to-person commercial solicitation of handicapped persons solely by virtue of their handicap. This law is not to be interpreted to restrict access by the public and press to information contained in public records. South Carolina Code 1976 §30-4-40.

Tennessee - The local government functions law provides that if a request is made for a copy of a public record that has commercial value and requires the reproduction of all or a portion of a computer generated map that was developed by an electronic system, the board of directors of the system may establish and impose reasonable fees for the reproduction relating to the actual development costs of the maps which may include: (1) labor costs, (2) costs incurred in design, development, testing, implementation and training, and (3) costs necessary to ensure that the map is accurate, complete and current. Once the total development costs have been recouped by the local government, the fees charged may only generate the amount necessary to maintain the data and ensure that it is accurate, complete and current for the life of the system. T.C.A. §7-52-135.

Another law allows certain clerks of the court to charge a fee not in excess of five dollars for computer searches for any public record having a commercial value. T.C.A. §8-21-408.

Yet another law provides that if a request is made for a copy of a public record that has commercial value and requires the reproduction of all or a portion of a computer generated map or other similar geographic data that was developed with public funds, the state department, agency or political subdivision that is responsible for the system may establish and impose reasonable fees for the reproduction relating to the actual development costs of the maps and may include the same elements as those listed above under T.C.A. §7-52-135. The development cost recovery is limited to not more than 10% of the total development costs unless additional development cost recovery between 10% and 20% is approved. T.C.A. §10-7-506. A "record that has commercial value" means a

record requested for any purpose other than a non-business use by an individual and a news gathering use by the news media. *Id.*

Texas - Under the Business and Commerce Code, the law provides that a person who has possession of crime victim or motor vehicle accident information that the person obtained or knows was obtained from a law enforcement agency may not use the information to contact a person who is a crime victim or who was involved in a motor vehicle accident or a member of the person's family for the purpose of soliciting business and may not sell the information to another person for financial gain. The attorney general may bring action against a person who violates this law. The violation is a class C misdemeanor unless the defendant has been previously convicted under this law more than two times, in which case the offense is a felony of the third degree. V.T.C.A., Bus. & C. §35.54.

C. The Implications Of Secondary Or Derivative Use Of Public Records On Access To Public Records

OPRA balances access and privacy through various exemptions which are based on privacy concerns, e.g. criminal investigatory records, victim's records, information received by a member of the Legislature from a constituent, information kept confidential pursuant to a court order, to name just a few. The Legislature has provided two additional mechanisms to add additional exemptions without the necessity of legislative amendments: Executive Order and Regulation. Each exemption from access represents a policy judgment that the interest in keeping information private outweighs any public benefit flowing from access.

There is growing concern over secondary or derivative use of personal information contained in accessible government records. This concern may be largely attributed to the computerization of federal and state governmental operations, including the electronic collection, processing, use and dissemination of its records. This very computerization of public records, which has made access to public records meaningful to greater numbers of citizens, has also generated concern that the information contained in government records can and will be utilized by companies combining it with other personal information from private sources to create, for example, profiles on consumers - commonly referred to as data-mining.⁹⁰ These private companies include credit card companies, credit reporting agencies, financial institutions, supermarkets, telephone companies, internet service companies and other retailers. These concerns, in turn, generate suggestions that "commercial use" of public records should be regulated and/or prohibited. These suggestions focus on the secondary or derivative use of the public record for purposes such as data-mining or consumer profiling which is perceived to be an abusive secondary or derivative use.

⁹⁰ This, at first blush, presents a paradox: create a system that allows government to function in secret or expose individuals to practices such as consumer profiling and data-mining. The Committee believes the solution is not, however, to sacrifice transparency in government by restricting access but, rather, to legislatively regulate certain secondary or derivative uses of information contained in public records.

Critical in defining what is a commercial use, however, is context. For example, the use of a name, photo or even a sketch in the context of a news story is not seen as a commercial appropriation use of that name, photo or sketch because of the context - a news story, even through a newspaper is a profit making commercial enterprise. In the context of the tort of privacy appropriation, the Restatement of the Law of Torts, Section 652(c) states:

“The value of the plaintiff’s name is not appropriated by mere mention of it, or by reference to it in connection with legitimate mention of his public activities.... The fact that the defendant is engaged in the business of publication, for example of a newspaper, out of which he makes a profit, is not enough to make the incidental publication a commercial use of the name or likeness.”

In short, context matters. As noted, at least some of the benefits that flow from a regime of public access to public records - research, economic growth - arise as a result of a secondary or derivative use of those public records which is commercial or profit based in nature. Any system, then, to alter the right of access to a record meeting the definition of government record in OPRA based upon a commercial secondary or derivative use of the record must, by definition, examine the context of that use. Such a regime would, however, have the effect of drastically altering the historical difference between the statutory right of access, now embodied in OPRA, and the common law right of access preserved by OPRA. In creating and maintaining these separate methods to access public records, New Jersey is unique among the states. In 1972, our Supreme Court in Irval Realty v. BPU Comm’rs, 61 N.J. 336 recognized the longstanding common law right of access to public records by stating:

“At common law a citizen had an enforceable right to require custodians of public records to make them available for reasonable inspection and examination. It was, however, necessary that the citizen be able to show an interest in the subject matter of the material he sought to scrutinize. Such interest need not have been purely personal. As one citizen or taxpayer out of many, concerned with a public problem or issue, he might demand and be accorded access to public records bearing upon the problem, even though his individual interest may have been slight. *Ferry v. Williams*, 41 N.J.L. 332 (Sup. Ct. 1879); *Taxpayers Association v. City of Cape May*, 2 N.J. Super. 27 (App. Div. 1949); *Moore v. Board of Chosen Freeholders of Mercer County*, 76 N.J. Super. 396 (App. Div. 1962), mod. 39 N.J. 26 (1962). Yet some showing of interest was required.”
[Irval, supra, at 372]

The Irval Court also noted that the common law right of access existed as an avenue separate and apart from the statutory right.

“A person seeking access to public records may today consider at least three avenues of approach. He may assert his common law right as a citizen to inspect public records; he may resort to the Right-to-Know Law, N.J.S.A. 47:1A-1 et seq., or, if he is a litigant, he may avail himself of the broad discovery procedures for which our rules of civil practice make ample provision.”
[Id.]

Prior to the passage of OPRA, there were two significant differences between the common law right of access and the statutory right of access. First, that the common law right of access encompassed, through its definition of a common law public record, a greater volume of records than the pre-OPRA Right-to-Know Law with its much more narrow definition of a public record. That distinction has largely been obliterated by OPRA's present definition of government record which essentially parallels the common law definition. Second, under the statutory right of access, if a record was a public record and not otherwise exempt under the statute, executive order or regulation, the record was available to the public, regardless of who sought the record and/or what use the requester wished to make of the record. North Jersey Newspapers v. Passaic County, 127 N.J. 9, 14 (1992). In short, there was no balancing of interest in the statutory right. The Legislature performed the balancing in the statute. This distinction persists.

The Legislature in OPRA clearly intended to preserve this second distinction between the common law right of access and the statutory right of access by preserving the common law right of access. N.J.S.A. 47:1A-8. However, adoption of a system that would limit or eliminate the right of access to records sought to be utilized for certain commercial purposes will inevitably lead to a system tantamount to the common law right of access, thereby obliterating the statutory right. This is so because it is not the record which creates the "commercial use", it is, rather, the secondary or derivative use of the record. It is then the context of that secondary or derivative use that will constitute the commercial use of the record. In order to ascertain the context of that secondary or derivative use of the record, custodians will be required to make inquiry of requestors. The inquiry will center on the purpose of the requestor and the intended use by the requestor in seeking the record. That purpose and intended use will be viewed through the prism of whatever definition of prohibited commercial use is included in the statute. This inquiry of the requestor by the custodian will inevitably transform the statutory right of access - historically marked by the absence of a necessity to define the purpose for which records are sought - into a common law right of access with an explanation to be given to the custodian by the requestor. This will have a profound chilling effect on the statutory right of access and is directly contrary to the entire structure of OPRA.

Consequently, any restrictions deriving from secondary or derivative uses of records cannot and should not result in legislation restricting access but, rather, such legislation should be directed at the perceived abuse either by increasing existing punishment, if present punishment is inadequate, or enacting legislation defining additional actions that will be deemed abusive and imposing punishment therefor.

D. Cost Of Access And Fees

Some have urged that many government records, particularly electronic government records, have a commercial value. There are those who propose that when the secondary or derivative use of a public record is a commercial/profit-making use, the government should be allowed to share in the profits. The advance the proposition that those who

stand to benefit from such derivative use of public records should be expected to contribute to the cost recovery of developing and maintaining such records. Those who advocate such a position recommend that such a fee should be likened to a user fee with those gaining financially from the use of public records helping to pay a portion of the development and maintenance costs. Such an argument was made in Florida in connection with its Open Public Records Act. The Florida Attorney General determined that providing access to public records is a statutory duty and should not be considered a revenue generating activity. 85-3 Opinion Fla. Attorney General 4 (1985). In a 1992 report, delivered after holding a series of public hearings on access to automated public records, the Florida Public Records Law Subcommittee concluded that the commercial value of a public record database and the requestor's motivation "are immaterial in determining access to that database and the fee(s) to be charged for access."⁹¹

The propriety of such a charge has not been decided in New Jersey under either the statutory right to know or the common law right to know. In Higg-A-Rella, Inc. v. County of Essex, 141 N.J. 35, 53 (1995), the Supreme Court observed:

"The Attorney General, in representing the Essex County Board of Taxation, reflects the State's legitimate interest in preserving the potential commercial value of the State's databases, even while serving the public's need for convenient access. The cost of computerization is substantial. Under both the Right-to-Know Law and the common law, the fee must be reasonable, and cannot be used as a tool to discourage access. Moore, supra, 39 N.J. at 31, 186 A.2d 676; Home News Publishing Co. v. Department of Health, 239 N.J. Super. 172, 182, 570 A.2d 1267 (App.Div.1990). Historically, a reasonable fee meant one that did not exceed the actual cost of copying. Moore, supra, 39 N.J. at 31, 186 A.2d 676. Plaintiff's thus assert that the fee for the computer tapes of the tax-assessment lists should reflect only the cost of the physical tape and the hours required to make the copy. The trial court disagreed, noting that 'the computer tapes represent a tremendous amount of data entry, at taxpayer expense. I see no reason why defendants should not decide whether they wish to sell it, and at what price.' 265 N.J. Super. at 625, 628 A.2d 392. The Appellate Division, however, in remanding this matter for a determination of a reasonable fee, effectively ordered that the fee reflect only the direct cost of copying the tapes, and not the cost of compiling them. 276 N.J. Super. at 191, 647 A.2d 862 ('The matter is remanded to the trial judge to determine the reasonable cost to prepare a duplicate list...on the particular electronic medium sought by plaintiffs.')."

The Court further stated:

"Defendants assert that limiting the fee to actual costs would violate the growing public policy of shifting the cost of developing and maintaining computerized public records from taxpayers generally to those who use them, and even profit from them, directly. According to defendants, such a limited fee structure would

⁹¹ See Final Report, Growth Management Data Network Coordinating Council, Public Records Law Subcommittee, Final Report 1992.

discourage further computerization. In *Techniscan*, supra, we addressed that issue, even though the plaintiff in that case sought computer printouts, and not electronic copies. We observed: ‘No party discussed whether the allowable costs of any requested copying were sufficient to the circumstances. The Legislature is considering further clarification of the relative interests of for-profit information-gathering services and public bodies.’ 113 N.J. at 237 n.1, 549 A.2d 1249.

We also note that the Legislature, in enacting and considering bills to update the State’s public-access law in a variety of areas, has consistently addressed the impact of technology on costs and fees. Section 1(a) of L.1994, c.54 authorizes the Administrative Office of the Courts to ‘develop and operate an automated data processing system that allows the public to access court information.’ Section 1(b) authorizes us to adopt fee schedules, and section 1(c) provides that the ‘proceeds collected...shall be deposited in the “Court Computer Information System Fund:...dedicated to the development, establishment, operation and maintenance of computerized court information systems in the judiciary.’”

[Id at 54]

The Court observed:

“Clearly, the public’s right to access to government information in this technological age presents complicated issues with wide-spread ramifications. Resolution of such major policy issues lies more properly with the Legislature. Ultimately, the Legislature must determine how and at what cost the public shall be entitled to receive electronic records. Until the Legislature acts in this field, however, courts must decide those issues. Hence, we remand to the trial court to determine what is a reasonable fee to charge plaintiffs for a copy of Essex County’s computer tape of the tax-assessment lists.”

[Id at 55]

Viewed in its proper perspective, the issue of costs of access and fees to be charged for those secondary or derivative uses of public records which yield commercial benefit to the user/requestor do not pose issues within the purview of the Privacy Study Commission. Simply put, the issues do not, in any true sense involve privacy issues. This question - a determination of at what cost the public shall be entitled to receive records - and whether there should be some enhanced charge depending on the secondary or derivative use of the records involved complex considerations, albeit not of a privacy nature. Clearly, the temptation must be avoided to establish rates that are punitive or represent a disincentive for public access. Public policy is not served by forcing those whose secondary or derivative use of public records is of a commercial but legitimate use out of business, either directly or indirectly. Whether there should be some value pricing - a recognition that classes of business users have different information needs and different resources - or some other mechanism should be the subject of a further study but it does not properly fall within the jurisdiction of the Privacy Study Commission and more particularly this Subcommittee.

SECTION 4: DATA PRACTICES SURVEY

EXECUTIVE SUMMARY

The New Jersey Privacy Study Commission administered its Data Practices Survey in October 2003 on a voluntary basis to almost 4,500 representatives of state and local government units and agencies in an effort to discern how personal information contained in government records is collected, processed, used and disseminated in the state of New Jersey. With a response rate of approximately 10%, the Commission was able to garner a glimpse into the data practices of these governmental organizations and analyze the results for a determination of how an individual's privacy interest in his or her personal information contained in government records is safeguarded in New Jersey.

The survey results indicate that the responding participating state and local government units and agencies in New Jersey overwhelmingly do not engage in data practices that violate an individual's privacy interest as it relates to the collection, processing, use and dissemination of personal information. However, the Commission is concerned that several data practices identified by a minority of the survey participants indicate that some records are not properly safeguarded which may result in a violation of an individual's privacy interest. These data practices are as follows:

- The use of personal information by some units or agencies for reasons other than those specified for its collection;
- The lack of a formal determination of whom within some units or agencies handle personal information;
- The unrestricted access to personal information in some units or agencies;
- The data mining of personal information by some units or agencies;
- The sharing of personal information with non-governmental third parties without obtaining consent from upper management or the person to whom the information pertains; and
- The selling, renting or leasing of personal information to non-governmental third parties by some units or agencies.

These data practices may be in violation of OPRA’s policy providing that a public agency has a responsibility and an obligation to safeguard a citizen’s personal information with which it has been entrusted from public access.

In an effort to determine and track the data practices of state and local government units and agencies, especially as it relates to the handling of personal information, the New Jersey Privacy Study Commission recommends that a scientifically developed and monitored data practices survey be administered every two years to a mandatory response population of state and local government units and agencies by the Department of State – Division of Archives and Records Management (DARM) or the Privacy Study Commission if this organization is adopted by the Governor or legislature as a permanent entity.

A. Introduction

One of the six subcommittees established by the New Jersey Privacy Study Commission (“Commission”) to carry out its legislative mandate “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...”⁹² is the New Jersey Data Practices Subcommittee. This subcommittee was specifically created to establish contacts in all state agencies and key local government professional organizations, develop and distribute a “data practices” survey to collect key information about how and why state and local government agencies collect, process, use and disseminate personal information, analyze the results of the data practices survey, and assess relevant privacy issues. This report was created by the Subcommittee and submitted to and accepted by the Commission.

The New Jersey Privacy Study Commission appreciates the efforts of the state and local government agencies and professional organizations in responding to the survey in a full and comprehensive manner. This document is intended to report on how the agencies responded to the Commission’s survey with editorial comment on what the survey results mean regarding the current data practices for handling personal information contained in government records in New Jersey.

⁹² N.J.S. 47:1A-15.

B. Recommendation

In an effort to determine and track the data practices of state and local government units and agencies, especially as it relates to the handling of personal information, the New Jersey Privacy Study Commission recommends that a scientifically developed and monitored data practices survey be administered every two years to a mandatory response population of state and local government units and agencies by the Department of State – Division of Archives and Records Management (DARM) or the Privacy Study Commission if this organization is adopted by the Governor or legislature as a permanent entity. The Commission believes that in doing so, the state will become better informed of how state and local government units and agencies are adhering to the policy in OPRA requiring that public agencies safeguard citizens’ personal information with which they are entrusted. Further, this mandatory survey may motivate agencies that are not in compliance with OPRA’s policy to safeguard personal information from public access to do so.

C. Survey Methodology

The Commission, with the assistance of the Department of State – Division of Archives and Records Management (“DARM”), developed a data practices survey consisting of six sections and thirty-six questions. The survey was divided into six sections as follows:

1. Participant Information (4 questions)
2. Data Collection (7 questions)
3. Data Processing and Storage (7 questions)
4. Data Use (7 questions)
5. Data Protection (6 questions)
6. Data Dissemination and Disclosure to Third Parties (5 questions).

The manner in which data is stored, protected, and disseminated in New Jersey is generally governed by DARM and the New Jersey Open Public Records Act (“OPRA”).⁹³ Applicable DARM statutes and regulations govern how records are stored, protected and destroyed, while OPRA governs the dissemination or disclosure of records. Specifically, DARM requires adherence to records retention schedules and maintains certification processes for the creation and use of data handling systems. Similarly, OPRA requires records custodians to disclose all government records unless the records are specifically exempted from such disclosure under OPRA, any other statute, resolution of either or both houses of the legislature, regulation promulgated under the authority of any statute or executive order of the Governor, executive order of the Governor, rules of court, any federal law, federal regulation or federal order.

The Data Practices Survey was administered in October 2003 on a voluntary basis to representatives of each of the 16 state departments (and their affiliated agencies), 21

⁹³ N.J.S.A. 47:1A-1 et seq.

counties, 566 municipalities, 615 school districts and 59 colleges and universities. More specifically, the survey was sent to those individuals within these organizations who handle personal information including state department personnel, state agency personnel, county clerks, county sheriffs, county surrogates (or attorneys), municipal clerks and administrators, municipal finance officers and tax collectors, local police and fire department personnel, fire district personnel, housing district personnel, school district personnel, and colleges and universities personnel.

The survey was completed by 483 respondents (a response rate of approximately 10%), including representatives from 12 state departments and their affiliated agencies, 20 counties, 132 municipalities, 33 school districts, and 5 colleges and universities.⁹⁴

D. Survey Results

1. Participant Information

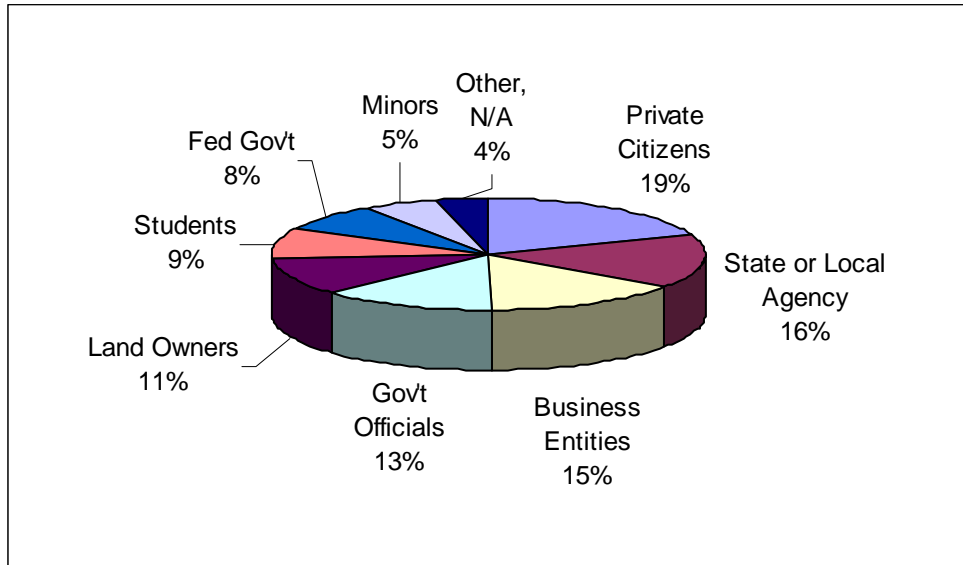
This section of the survey asked four questions relevant to the identity of the voluntary participants and their operating organizations. Specifically, the survey asked the voluntary participants to provide their name, the public agency they represent, the title or function of their unit or agency, and the type of customers their unit or agency serve.

Private Citizens are the Main Customers of Units or Agencies

According to the survey results, most respondents indicated that private citizens are the customers served by their units or agencies, followed by (in the order of the most responses to the least responses): (1) other state or local government agencies (including personnel within their own unit or agency), (2) business entities, (3) government officials, (4) land owners, (5) students, (6) the federal government, and (7) minor children. See Graph 1. Also see Appendix B for the “other” responses given by survey participants for Participant Information – Question 4.

⁹⁴ The survey response rate is based on an approximation of the entire universe of potential participants who were asked to complete the survey, including at least one representative from each of the following groups of state and local government personnel: 228 state department divisions (units) and agencies, 21 county clerks, 21 county sheriffs, 21 county surrogates (or attorneys), 566 municipal clerks, 566 municipal administrators, 566 municipal finance officers, 566 municipal tax collectors, 566 municipal police chiefs, 566 municipal fire chiefs, 182 fire district personnel, 211 housing district personnel, 616 school district administrators, and 57 colleges and universities personnel. Thus, the total survey population could have been as many as 4,483 individuals or more. Because the requests to complete the surveys were delivered to the survey population primarily by e-mail, it cannot be determined with complete accuracy the exact number of individuals who received the request.

GRAPH 1:
(Question 4. Who are the customers of your unit or agency?)



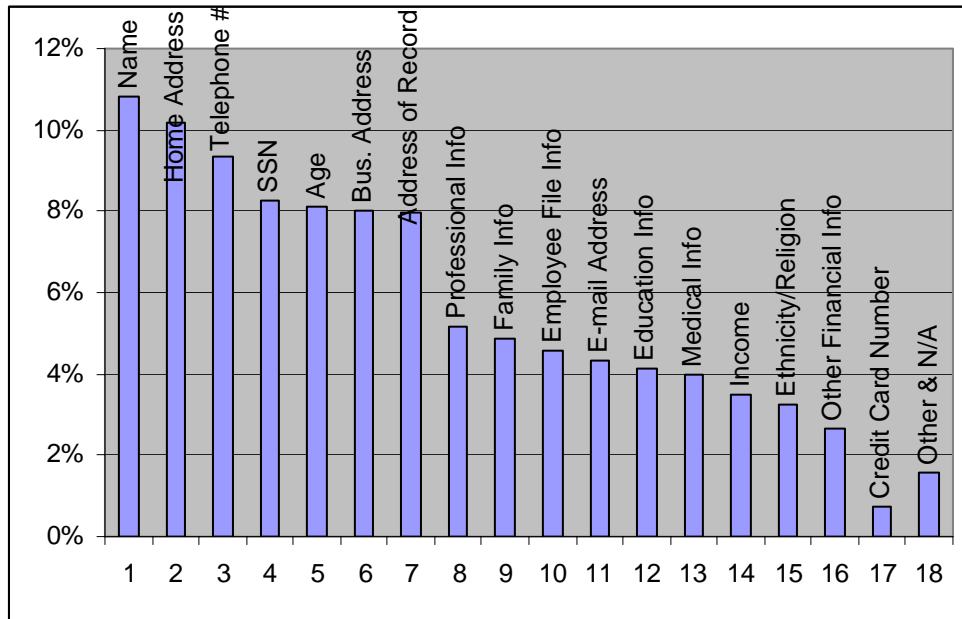
2. Data Collection

This section of the survey asked seven questions relevant to the methods used to collect personal information, the types and sources of personal information collected, whom within the unit or agency collects personal information, and the reasons personal information is collected.

Types of Personal Information Collected

According to the survey results, most participants indicated that the following types of personal information is collected by their units or agencies (in the order of the most responses to the least responses): (1) name, (2) home address, (3) home telephone number, (4) social security number, (5) age or date of birth, (6) business address, (7) address of record, (8) professional information (9) family information, (10) employee file information, (11) e-mail address, (12) education information, (13) medical information, (14) income, (15) ethnicity or religious affiliation, (16) other financial information, and (17) credit card number. See Graph 2. Also see Appendix B for the “other” responses given by survey participants for Data Collection – Question 2.

GRAPH 2:
(Question 2. Identify the types of personal information your agency collects.)



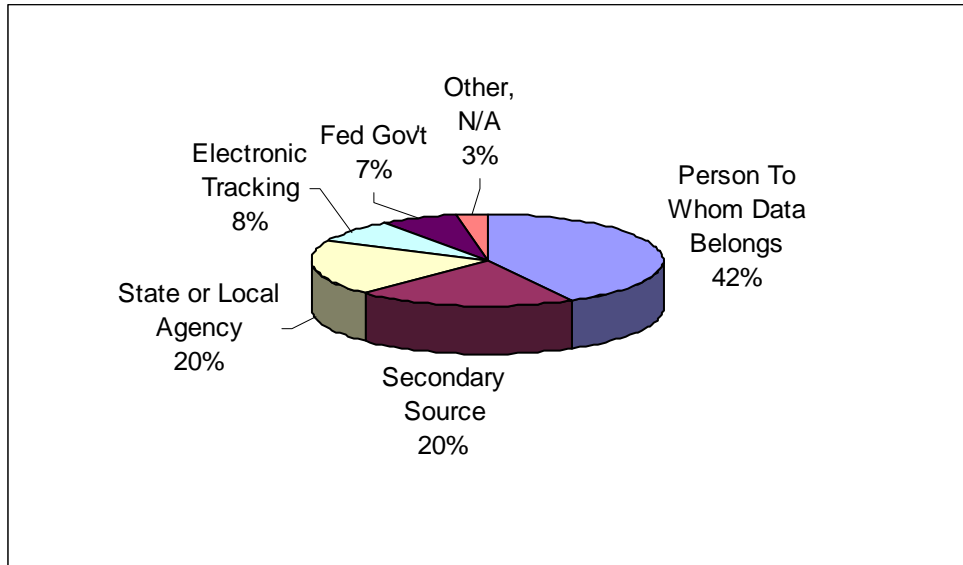
Personal Information is Collected from Individuals “In Person”

The survey results also indicated that personal information is most often collected from customers and other agency users “in person,” followed by these other methods of collection (in the order of the most responses to the least responses): (1) mail, (2) hard-copy form or application, (3) telephone, (4) fax, (5) e-mail, and (6) internet form or application. See Appendix B for the “other” responses given by survey participants for Data Collection – Question 1.

Personal Information is Collected from the Person to Whom the Data Pertains

The survey results further indicated that the person to whom the data pertains is the primary source of the personal information collected. Other sources signified by the survey participants (in the order of the most responses to the least responses) are as follows: (1) secondary sources such as a guardian or lawyer, (2) another state or local government agency, (3) an electronic tracking system, and (4) the federal government. Sixty respondents indicated that their units or agencies have an accuracy verification process for personal information collected from secondary sources. See Graph 3. Also see Appendix B for the “other” responses given by survey participants for Data Collection – Question 3.

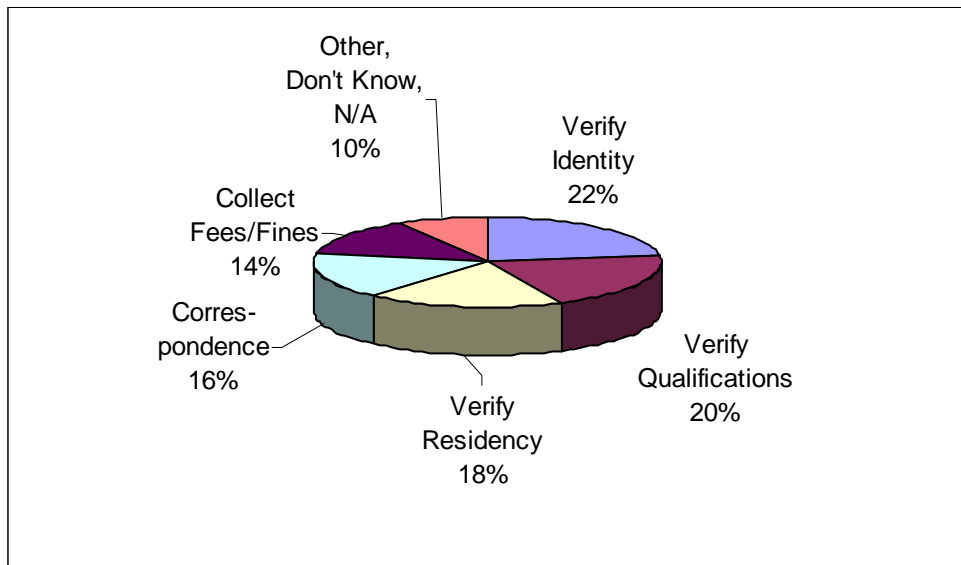
GRAPH 3:
(Question 3. Identify the source from which personal information is collected.)



Personal Information is Collected to Verify Identity

Most survey participants indicated that their units or agencies collect personal information to verify identity. Other reasons for collecting personal information (in the order of the most responses to the least responses) were: (1) to verify qualifications (for benefits, employment, licensure, registration, etc.), (2) to verify residency, (3) for correspondence purposes, and (4) to collect fees and fines. See Graph 4. Also see Appendix B for the “other” responses given by survey participants for Data Collection – Question 5.

GRAPH 4:
(Question 5. What are the reasons that your agency collects personal information?)



Public Agencies Advise Customers of the Reasons They Are Collecting Data

Also according to the survey results, participants overwhelmingly indicated that their unit or agency advises the person to whom the data pertains of the reason they collect the data and how the data will be used. The survey participants also indicated that a wide range of personnel within their units and agencies collect personal information varying from secretaries to department heads.

3. Data Processing and Storage

This section of the survey asked seven questions relevant to how personal information that is collected is processed, stored, and disposed. Additionally, this section asked participants about their organization’s adherence to state regulations regarding certified records destruction requirements, image or scanning systems certification requirements, and retention schedule requirements for records containing personal information.

Personal Information is Processed, Stored and Destroyed In-House

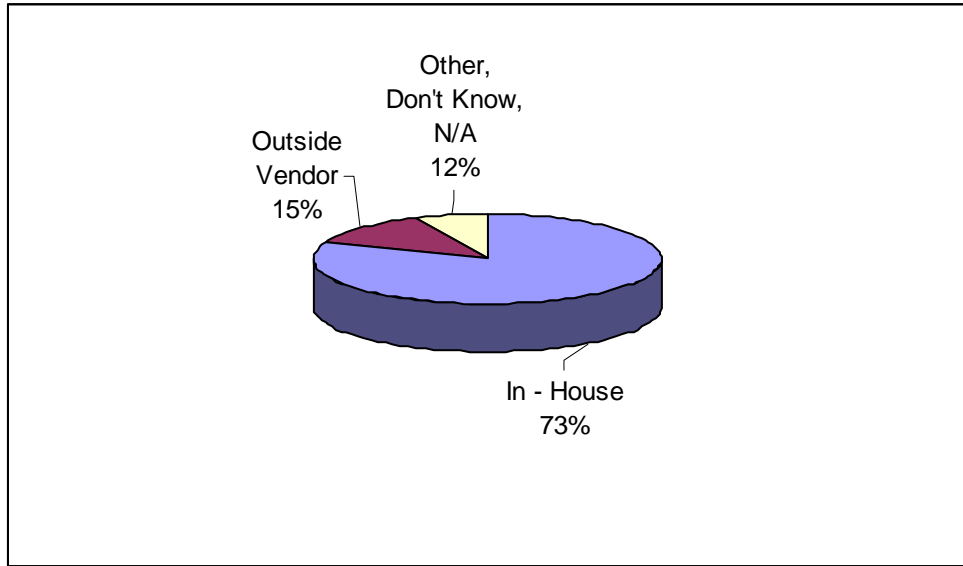
The survey results overwhelming indicate that personal information is processed, stored and destroyed (including shredding) in-house, as opposed to being outsourced to non-governmental vendors or contractors. However, most outside vendors are used for record destruction (112 out of 483 responses) than for record storage (76 out of 483 responses) or data processing (72 out of 483 responses). See Graph 5 (illustrates the results of questions 8, 9, and 10 combined). Also see Appendix B for the “other” responses given by survey participants for Data Processing and Storage – Questions 8, 9, and 10.

GRAPH 5:

(Question 8. Data is processed...)

(Question 9. Data or records are stored by...)

(Question 10. Disposal, destruction and shredding of records are done...)

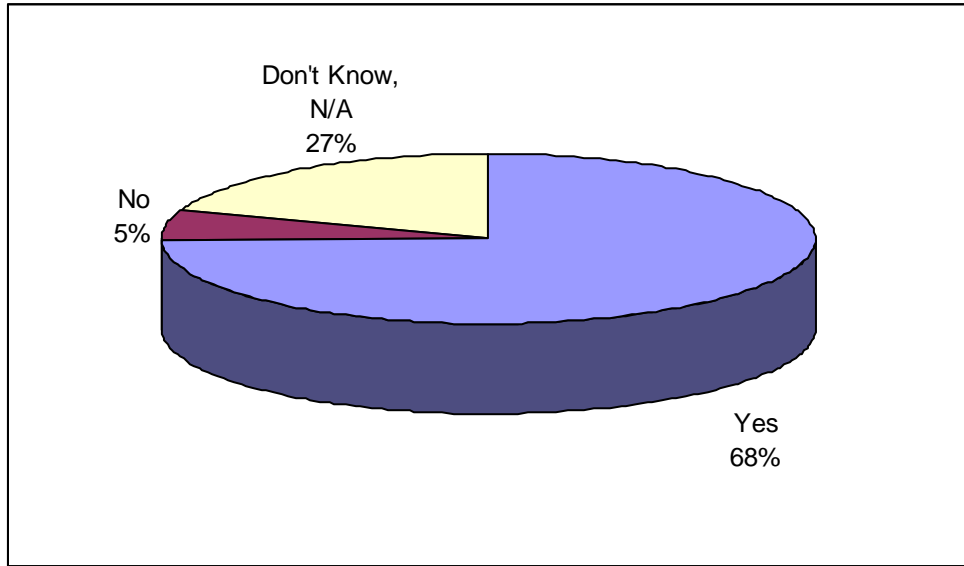


Public Agencies Adhere to State Regulations for the Certified Destruction of Government Records

According to the survey results, most participants indicated that their units or agencies adhere to state regulations regarding the certified destruction of records containing personal information than those that do not. However, a number of the participants (85 out of 483 responses) did not know if their units or agencies adhere to these regulations and some indicated that their units or agencies do not adhere to the regulations (26 out of 483 responses). See Graph 6. Also see Appendix A for the objective responses given by survey participants for Data Processing and Storage – Question 11.

GRAPH 6:

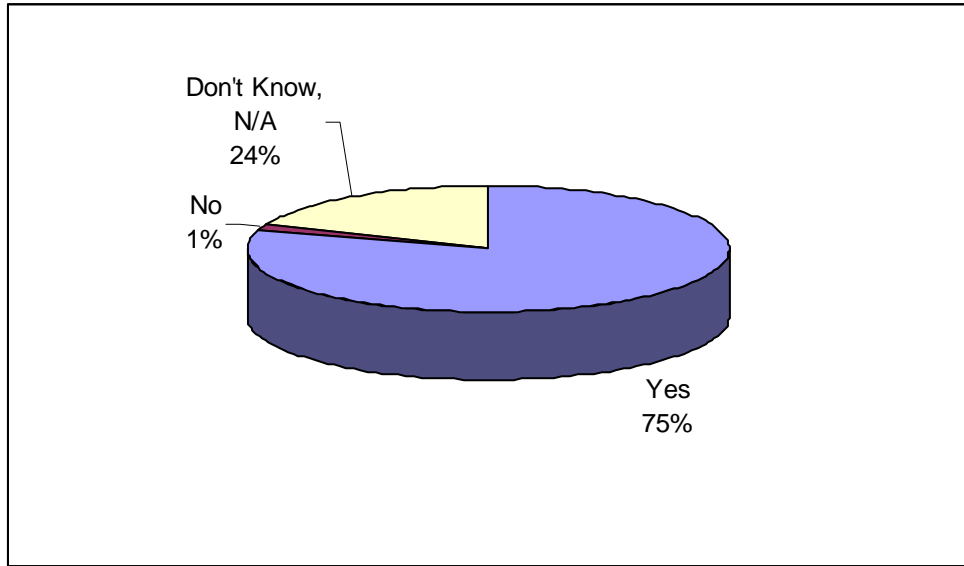
(Question 11. Does your agency use certified destruction of records containing personal information as prescribed by the Department of State - Division of Archives and Records Management?)



Also according to the survey results, most participants indicated that their units or agencies adhere to the state's requirements for approval of disposal or destruction of records than those that do not. However, a number of survey participants (86 out of 483 responses) did not know if their units or agencies adhere to these requirements and only a few indicated that their units or agencies do not adhere to the requirements (7 responses). See Graph 7. Also see Appendix A for the objective responses given by survey participants for Data Processing and Storage – Question 12.

GRAPH 7:

(Question 12. Does your agency adhere to the state’s requirements for approval of disposal or destruction of records by the Department of State – Division of Archives and Records Management?)

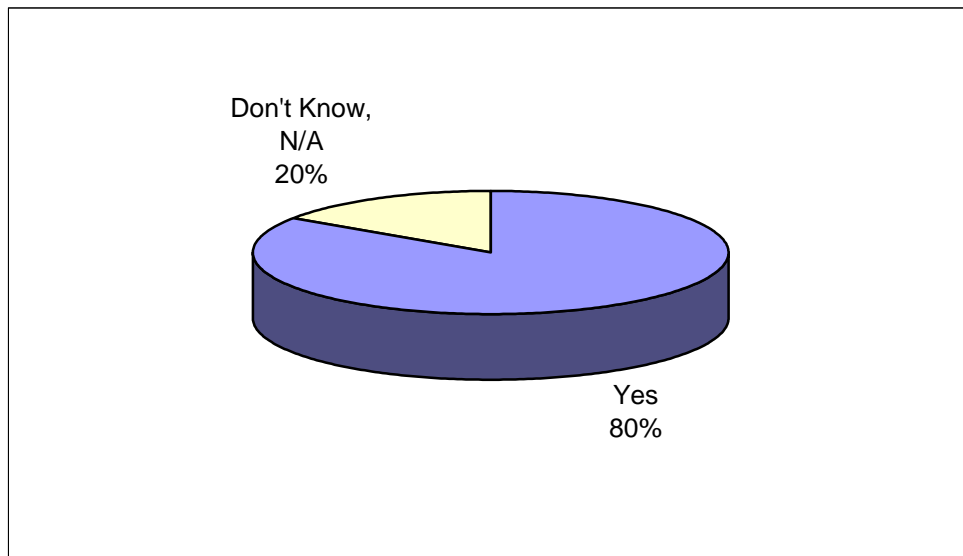


Public Agencies Adhere to the State’s Records Retention Schedules

Most survey participants indicated that their units or agencies adhere to the state’s records retention schedules than those that do not. However, a number of participants (71 out of 483 responses) did not know if their units or agencies adhere to the retention schedules and one participant indicated that his or her unit or agency does not adhere to them. See Graph 8. Also see Appendix A for the objective responses given by survey participants for Data Processing and Storage – Question 14.

GRAPH 8:

(Question 14. Does your agency adhere to the state’s records retention schedules for all records containing personal information?)



Certification of Image or Scanning Systems is Not Relevant for Most Public Agencies

The survey participants overwhelmingly responded that certification of their organization’s image or scanning systems was not relevant, presumably because they do not have such systems in place. See Appendix A for the objective responses given by survey participants for Data Processing and Storage – Question 13.

4. Data Use

This section of the survey asked seven questions regarding the purposes for which personal information is used, the restrictions on access to such information within the units or agencies, the determination of whom within the units or agencies handle the personal information, sharing of the personal information, and data mining of the personal information.

Personal Information is Used for Identification Purposes

According to the survey results, most participants indicated that personal information is used by their units or agencies for identification purposes. The survey participants further indicated that personal information is also used by their organizations for the following purposes (in the order of the most responses to the least responses): (1) communication or correspondence, (2) request for services or benefits, (3) registration, (4) licensure, and (5) human resource issues. See Appendix B for the “other” responses given by survey participants for Data Use – Question 15.

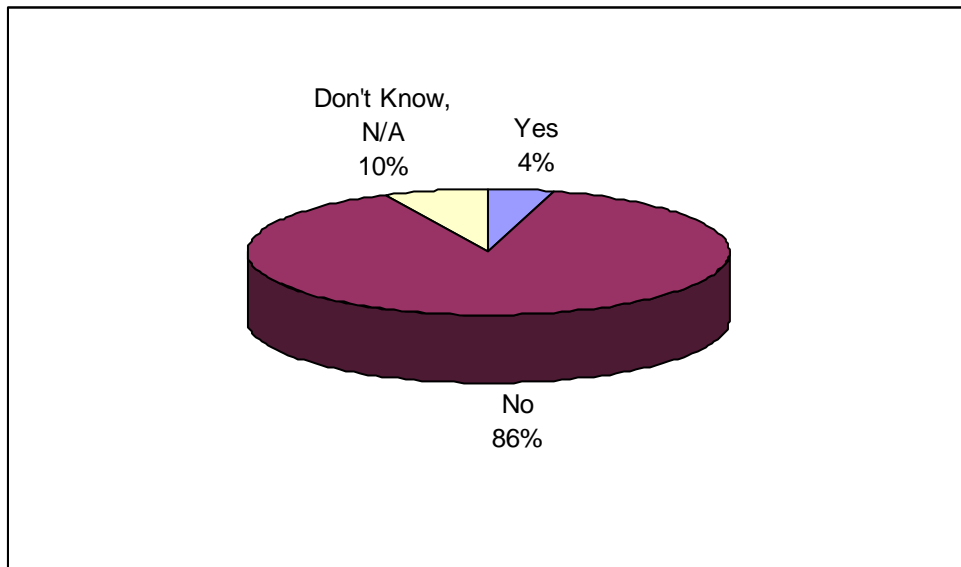
Personal Information is Used Only for the Reasons Specified

The survey participants also overwhelmingly indicated that the personal information their units or agencies collect is not used for purposes other than those specified as the reasons

it is collected. However, a number of participants (21 out of 483 responses) indicated that personal information is used for reasons other than those specified. See Graph 9. Also see Appendix A for the objective responses given by survey participants for Data Use – Question 18.

GRAPH 9:

(Question 18. Is personal information used for purposes other than those specified as the reasons for its collection?)



Access to Personal Information Within Public Agencies is Based on Job Function

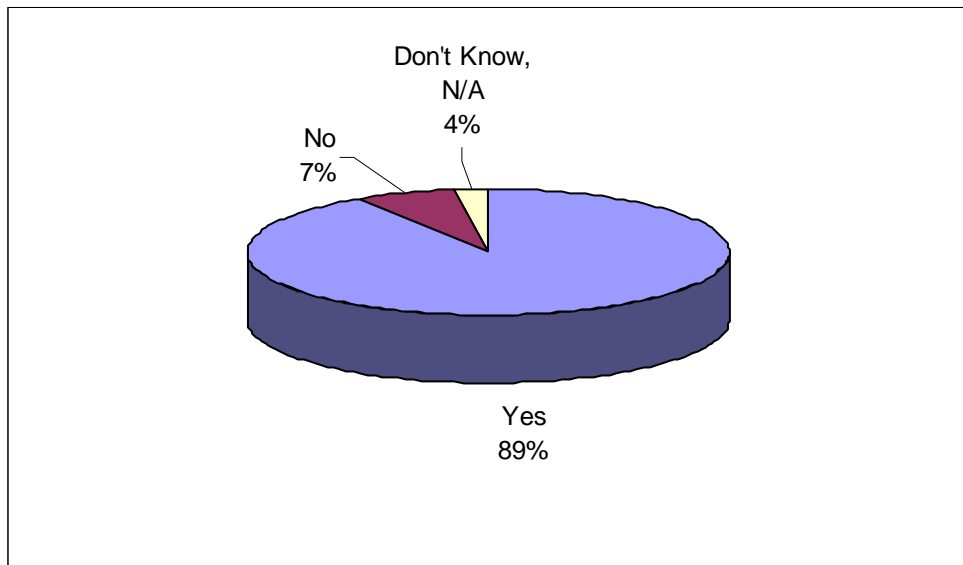
Most survey participants indicated that there is a formal determination of whom within their units or agencies handles the personal information they collect according to job function. However, a number of participants (53 out of 483 responses) indicated that there was no formal process or determination of whom within their units or agencies handles the personal information they collect. Survey participants also indicated (in order of the most responses to the least responses) that this determination is also made by job title and supervisor level. See Appendix B for the “other” responses given by survey participants for Data Use – Question 17.

Access to Personal Information Within Public Agencies is Restricted

The survey participants overwhelmingly indicated that access to personal information collected by their unit or agency is restricted to those persons within their organization who use the data in the performance of their job functions. However, a number of participants (32 out of 483 responses) indicated that access to this information is not restricted. See Graph 10. Also see Appendix A for the objective responses given by survey participants for Data Use – Question 16.

GRAPH 10:

(Question 16. Is access to personal information restricted to those persons within the agency who use the data in the performance of their job functions?)

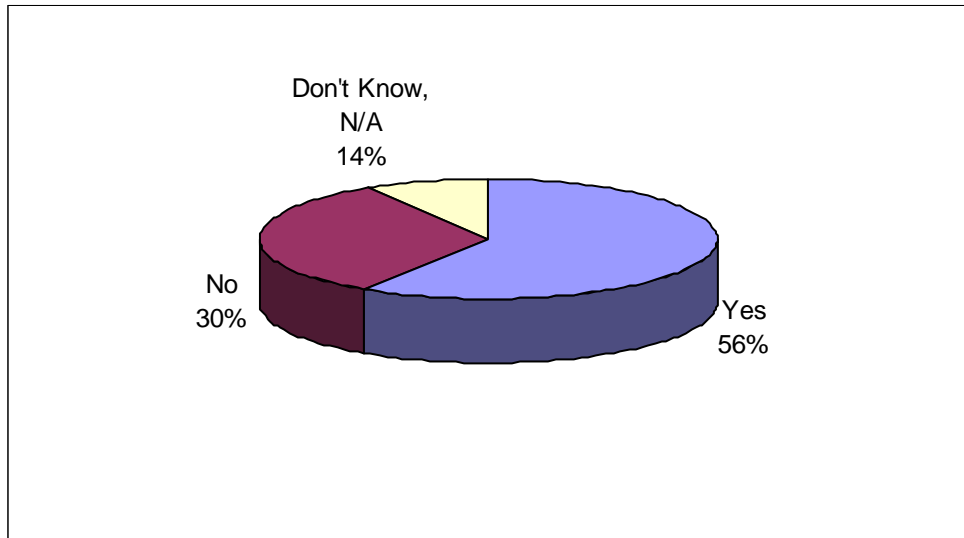


**Most Public Agencies Share Personal Information with Other Government Agencies
But Only Some Engage in Data Mining**

Most survey participants indicated that their units or agencies share personal information they collect with other federal, state and local government agencies. See Graph 11. Also see Appendix A for the objective responses given by survey participants for Data Use – Question 19. Survey participants were almost evenly divided on the issue of whether their units or agencies obtain consent to share personal information with other agencies (when not mandated by law). See Appendix A for the objective responses given by survey participants for Data Use – Question 20.

GRAPH 11:

(Question 20. Does your agency obtain consent to share personal information with other agencies (if not mandated by law)?)

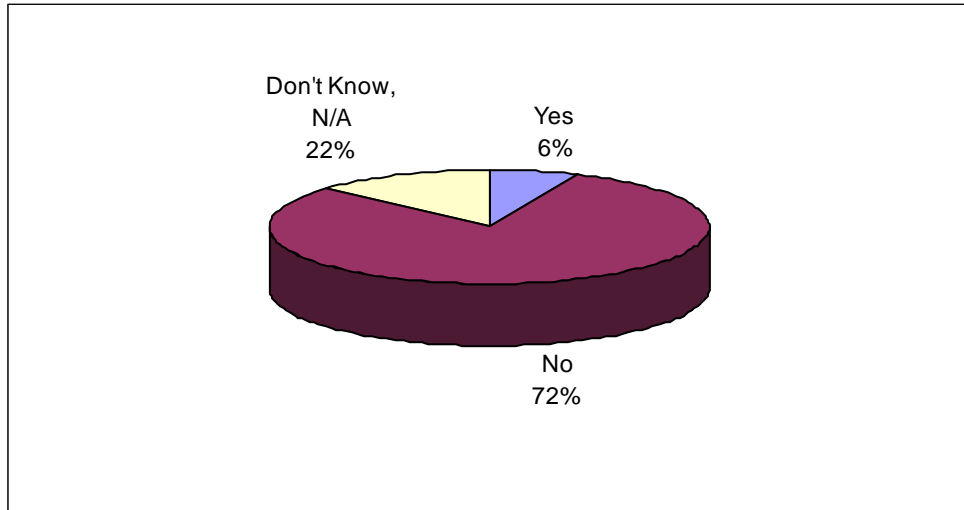


Some survey participants (29 out of 483 responses) indicated that their units or agencies engage in “data mining” of personal information.⁹⁵ However, the overwhelming majority (348 responses) indicated that their units or agencies do not engage in data mining. See Graph 12. Also see Appendix A for the objective responses given by survey participants for Data Use – Question 21.

⁹⁵ Data mining is the analysis of data in a database using tools that look for trends or anomalies without knowledge of the meaning of the data. (The Free On-Line Dictionary of Computing, 1993 – 2004 Dennis Howe) For example, some agencies may collect personal information and combine it with data obtain from other sources (both governmental and non-governmental), and then “mine” the data to reveal patterns and trends that were not previously obvious or intended by the individuals who provided the personal information.

GRAPH 12:

Question 21. Does your agency engage in “data mining” of personal information?)



5. Data Protection

This section of the survey asked six questions regarding how units and agencies ensure data is accurate, complete and up-to-date, as well as whether personal information is protected, whether the safeguards are enforced and communicated throughout the organization, and whether agencies educate employees on the personal information that is exempt under OPRA.

Safeguards to Protect Personal Information are Enforced and Communicated

According to the survey results, participants overwhelmingly indicated that their units or agencies protect personal information against risk of loss or unauthorized access. However, a number of participants (11 out of 483 responses) indicated that their units or agencies do not. Also, the survey participants overwhelmingly indicated that the safeguards implemented by their organizations to protect personal information are enforced and communicated throughout their organizations. The survey participants also indicated that their organizations educate employees (including temporary employees) on the types of personal information that are exempt from disclosure under OPRA.⁹⁶ See Appendix A for the objective responses given by survey participants for Data Protection – Questions 23 and 25 - 27.

⁹⁶ OPRA specifically exempts from disclosure the following personal information: social security numbers, credit card numbers, unlisted telephone numbers and drivers license numbers. N.J.S.A. 47:1A-1.1.

6. Data Dissemination and Disclosure to Third Parties

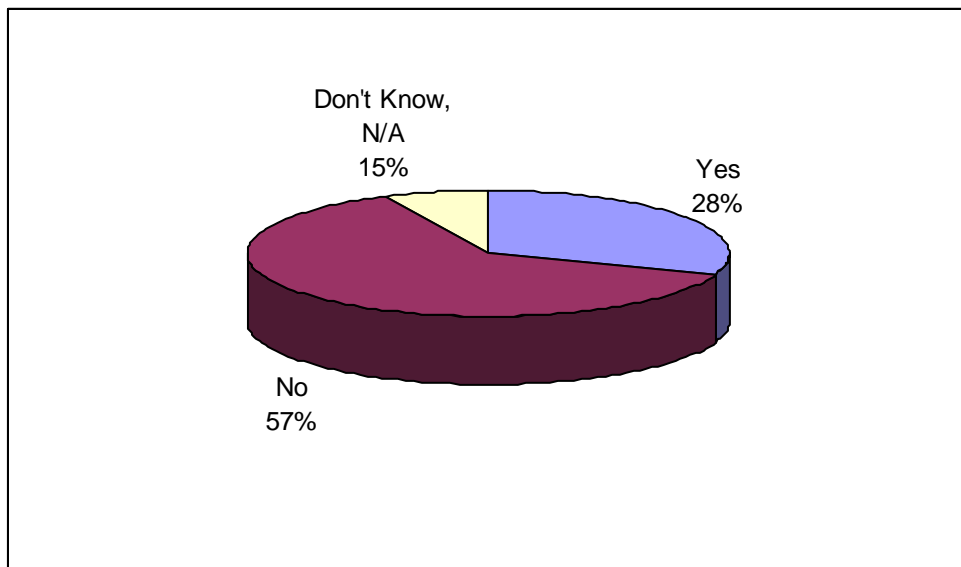
The final section of the survey asked five questions relevant to whether the participants' units or agencies share personal information with non-governmental third parties, whether consent is obtained to engage in such sharing, and whether organizations sell personal information to non-governmental third parties.

Public Agencies Do Not Generally Share Personal Information Outside of the Government

According to the survey results, most participants indicated that their units or agencies do not share personal information with third parties outside of the federal, state and local governments. However, some participants (133 out of 483 responses) indicated that their organizations do engage in such activity. See Graph 13. Also see Appendix A for the objective responses given by survey participants for Data Dissemination and Disclosure to Third Parties – Question 28.

GRAPH 13:

(Question 28. Does your agency share personal information with third parties outside of federal, state and local government?)



Some survey participants (59 out of 483 responses) indicated that they engage in this disclosure of personal information to non-governmental third parties without obtaining consent from upper management or the person to whom the information pertains. See Appendix A for the objective responses given by survey participants for Data Dissemination and Disclosure to Third Parties – Question 30.

The survey participants overwhelmingly indicated that their units or agencies do not sell, rent, or lease personal information. However, some participants (6 out of 483 responses) indicated that their organizations do. See Appendix A for the objective responses given

by survey participants for Data Dissemination and Disclosure to Third Parties – Question 31.

E. Conclusion

The New Jersey Privacy Study Commission administered the Data Practices Survey on a voluntary basis to representatives of state and local government agencies in an effort to discern how personal information is collected, processed, used and disseminated in the state of New Jersey. Based on the survey responses, the Commission concludes that the following are the data practices of state and local government units and agencies in New Jersey:

Data Collection

- Private citizens are the main customers of public agencies;
- Name, home address, home telephone number, social security number, age or date of birth, business address, and address of record are the most frequently requested personal information by public agencies;
- Personal information is most frequently collected from individuals in person and from the person to whom the data pertains;
- Personal information is most often collected to verify identify;
- Public agencies advise their customers of the reasons the personal information is collected;

Data Processing and Storage

- Personal information is processed, stored and destroyed in-house as opposed to by outside, non-governmental vendors;
- Public agencies adhere to state regulations for the certified destruction of government records and the state's records retention schedules;
- Certification of image or scanning systems is not relevant for most public agencies (presumably because most agencies do not have such systems in place);

Data Use

- Personal information is most often used for identification purposes;
- Public agencies do not use personal information for purposes other than those specified as the reasons it is collected;
- Access to personal information within public agencies is based on job functions and is restricted;
- Most public agencies share personal information with other federal, state and local government agencies;
- Some public agencies engage in data mining;

Data Protection

- Safeguards to protect personal information exist and are enforced and communicated within public agencies;

Data Dissemination and Disclosure to Third Parties

- Public agencies do not generally share personal information with non-governmental third parties.

The survey results indicate that participating state and local government agencies in New Jersey overwhelmingly do not engage in data practices that may violate an individual's privacy interest as it relates to the collection, processing, use and dissemination of personal information. However, the Commission is concerned that several data practices identified by a minority of the survey participants indicate that some records are not properly safeguarded which may result in a violation of an individual's privacy interest. These data practices are as follows:

- The use of personal information by some units or agencies for reasons other than those specified for its collection (21 responses);
- The lack of a formal determination of whom within some units or agencies handle personal information (53 responses);
- The unrestricted access to personal information in some units or agencies (32 responses);
- The data mining of personal information by some units or agencies (29 responses);
- The sharing of personal information with non-governmental third parties (133 responses) without obtaining consent from upper management or the person to whom the information pertains (59 responses); and
- The selling, renting or leasing of personal information to non-governmental third parties by some units or agencies (6 responses).

These data practices may be in violation of OPRA's policy providing that a public agency has a responsibility and an obligation to safeguard a citizen's personal information with which it has been entrusted from public access.⁹⁷

In an effort to determine and track the data practices of state and local government units and agencies, especially as it relates to the handling of personal information, the New

⁹⁷ N.J.S.A. 47:1A-1.

Jersey Privacy Study Commission recommends that a scientifically developed and monitored data practices survey be administered every two years to a mandatory response population of state and local government units and agencies by the Department of State – Division of Archives and Records Management (DARM) or the Privacy Study Commission if this organization is adopted by the Governor or legislature as a permanent entity. The Commission believes that in doing so, the state will become better informed of how state and local government units and agencies are adhering to the policy in OPRA requiring that public agencies safeguard citizens’ personal information with which they are entrusted. Further, this mandatory survey may motivate agencies that are not in compliance with OPRA’s policy to safeguard personal information from public access to do so.

SECTION 5: CONCLUSION

The Commission believes that the policy recommendations for administrative and legislative action contained in this report strike an appropriate balance between the needs for openness and the transparency of government and the citizens' reasonable expectation of privacy in their personal information contained in government records.

APPENDIX A
Data Practices Survey Results:
RESPONSES TO OBJECTIVE QUESTIONS

PARTICIPANT INFORMATION

(The following information is required to complete the survey.)

1. Name

2. Which public agency do you represent?

A. Department

Department of Banking & Insurance = 8 Responses
Department of Commerce = 2 Responses
Department of Community Affairs = 19 Responses
Department of Corrections = 45 Responses
Department of Education = 5 Responses
Department of Environmental Protection = 7 Responses
Department of Health & Senior Services = 9 Responses
Department Human Services = 16 Responses
Department of Military & Veteran Affairs = 19 Responses
Department of Personnel = 7 Responses
Department of Transportation = 17 Responses
Department of Treasury = 46 Responses

(4 departments did not respond)

B. Division

C. Unit or Agency

D. County

20 out of 21 Counties Responded

E. Municipality

132 out of 566 Municipalities Responded

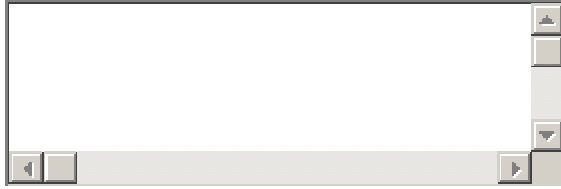
F. School District

33 out of 615 School Districts Responded

G. College or University

5 out of 59 Colleges Responded

3. What is the title and function(s) of your unit or agency?



4. Who are the customers of your unit or agency? (check all that apply):

- | | |
|--|---|
| <input type="checkbox"/> A. Other state or local government agencies (including other personnel within your unit or agency)
323 Responses | <input type="checkbox"/> B. Government officials
263 Responses |
| <input type="checkbox"/> C. Private citizens
385 Responses | <input type="checkbox"/> D. Land owners
214 Responses |
| <input type="checkbox"/> E. Students
187 Responses | <input type="checkbox"/> F. Minor children
111 Responses |
| <input type="checkbox"/> G. Business entities
296 Responses | <input type="checkbox"/> H. Federal government
158 Responses |
| <input type="checkbox"/> Other <input type="text"/>
78 Responses | <input type="checkbox"/> N/A
6 Responses |

SURVEY

("Agency" includes your unit or office)

DATA COLLECTION

1. Identify your agency's methods of collecting personal information from customers and other agency users (check all that apply):

- | | |
|---|--|
| <input type="checkbox"/> A. In person
403 Responses | <input type="checkbox"/> B. Telephone
338 Responses |
| <input type="checkbox"/> C. Mail
388 Responses | <input type="checkbox"/> D. Orally
290 Responses |
| <input type="checkbox"/> E. Facsimile
333 Responses | <input type="checkbox"/> F. Hard-copy form or application
387 Responses |
| <input type="checkbox"/> G. Internet form or application
147 Responses | <input type="checkbox"/> H. E-mail
238 Responses |

Other
26 Responses

N/A
14 Responses

2. Identify the types of personal information your agency collects (check all that apply):

A. Name
466 Responses

B. Social Security Number
356 Responses

C. Home Address
438 Responses

D. Home Telephone Number
401 Responses

E. Business Address
344 Responses

F. Address of Record
343 Responses

G. Age or Date of Birth
349 Responses

H. Ethnicity or Religious affiliation
140 Responses

I. Employee File Information
197 Responses

J. Credit Card Number
31 Responses

K. Income
151 Responses

L. Other Financial Information
115 Responses

M. Family Information
210 Responses

N. Education Information
178 Responses

O. Professional Information
222 Responses

P. Medical Information
172 Responses

Q. E-mail Address
186 Responses

Other
57 Responses

N/A
11 Responses

3. Identify the source from which personal information is collected (check all that apply):

A. The person to whom the data pertains
452 Responses

B. An electronic tracking system
85 Responses

C. A secondary source (guardian, lawyer, etc.)
219 Responses

D. Other state or local government agency
213 Responses

E. Federal government
77 Responses

F. There is an accuracy verification process for personal information collected from secondary sources

60 Responses

Other

31 Responses

N/A

11 Responses

4. Identify, by job title or position only, those within your agency who collect personal information (List one job title or position per line):

A. See responses in separate report.

B. See responses in separate report.

C. See responses in separate report.

D. See responses in separate report.

E. See responses in separate report.

F. There are many more not listed

91 Responses

I do not know

5 Responses

N/A

17 Responses

5. What are the reasons that your agency collects personal information? (check all that apply):

A. To verify identity

340 Responses

B. To verify residency

278 Responses

C. To verify qualifications (for benefits, employment, licensure, registration etc.)

307 Responses

D. To cross reference with other government records

132 Responses

E. To collect fees and fines (other account information)

206 Responses

F. For correspondence purposes

249 Responses

Other

125 Responses

I do not know

1 Response

N/A

12 Responses

6. Does your agency need all of the personal information that it collects to perform its functions? (For example, could your agency perform a visual verification of a customer's driver license and indicate that the residency was confirmed by agency personnel in lieu of requiring the customer's home address appear on the form or application?)

Yes 331 Responses No 100 Responses I do not know 52 Responses

7. Before or at the time your agency collects personal information, does it advise the person to whom the data pertains of the following (check all that apply):

- A. The reason for collection of the data Yes 387 Responses No 96 Responses
- B. How the data will be used Yes 342 Responses No 137 Responses

DATA PROCESSING AND STORAGE

8. Data is processed (check all that apply):

- A. In-house 466 Responses
- B. By outside vendor or contractor 72 Responses
- Other 38 Responses
- I do not know 4 Responses
- N/A 6 Responses

9. Data or records are stored (check all that apply):

- A. In-house 471 Responses
- B. By an outside vendor 76 Responses
- Other 73 Responses
- I do not know 4 Responses
- N/A 4 Responses

10. Disposal, destruction and shredding of records are done (check all that apply):

- A. In-house 380 Responses
- B. By an outside vendor 112 Responses
- Other 36 Responses
- I do not know 22 Responses
- N/A 31 Responses

11. Does your agency use certified destruction of records containing personal information as proscribed by the Department of State (Division of Archives and Records Management)?

- Yes 328 Responses
- No 26 Responses
- I do not know 85 Responses
- N/A 44 Responses

12. Does your agency adhere to the state's requirements for approval of disposal or destruction of records by Department of State (Division of Archives and Records Management)?

- Yes 359 Responses
- No 7 Responses
- I do not know 84 Responses
- N/A 33 Responses

13. If you image or scan your records, is the system certified by the State Records Committee?

- Yes 48 Responses
- No 26 Responses
- I do not know 73 Responses
- N/A 336 Responses

14. Does your agency adhere to the state's records retention schedules for all records containing personal information?

information?

Yes 384 Responses No 1 Response I do not know 71 Responses N/A 27 Responses

DATA USE

15. Indicate the purposes for which personal information is used by your agency (check all that apply):

A. Identification
385 Responses

B. Registration
216 Responses

C. Licensure
210 Responses

D. Request for services or benefits
246 Responses

E. Human Resources
204 Responses

F. Communication or correspondence
312 Responses

Other
107 Responses

I do not know
0 Response

N/A
11 Responses

16. Is access to personal information restricted to those persons within the agency who use the data in the performance of their job functions?

Yes 428 Responses No 32 Responses I do not know 10 Responses N/A 13 Responses

17. How is it determined whom within the agency handles personal information collected by the agency? (check all that apply):

A. By job *Title*
224 Responses

B. By supervisor *Level*
164 Responses

C. By job *function*
347 Responses

D. There is no formal process or determination of whom within the agency handles the personal information the agency collects
53 Responses

Other
10 Responses

I do not know
6 Responses

N/A
14 Responses

18. Is personal information used for purposes other than those specified as the reasons for its collection?

Yes 21 Responses No 413 Responses I do not know 33 Responses N/A 16 Responses

19. Does your agency share personal information with other federal, state and local government agencies?

Yes 270 Responses No 146 Responses I do not know 41 Responses N/A 26 Responses

20. Does your agency obtain consent to share personal information with the other agencies (if not mandated by law)?

Yes 144 Responses No 122 Responses I do not know 71 Responses N/A 146 Responses

21. Some agencies may collect massive amounts of personal information from individuals, and combine it with data obtained from other sources (i.e., other governmental agencies or non-governmental organizations). Then, the data is "mined" to reveal patterns and trends that were not previously obvious.

Does your agency engage in "data mining" of personal information?

Yes 29 Responses No 348 Responses I do not know 58 Responses N/A 48 Responses

DATA PROTECTION

22. Please describe how your agency ensures data is accurate, complete, and up-to-date: (If you get no such assurance, please write "N/A" in the text box)

See responses in separate report.

23. Does your agency protect personal information against risks of loss or unauthorized access?

Yes 420 Responses No 11 Responses I do not know 31 Responses N/A 21 Responses

24. If so, are the safeguards manual or electronic (check all that apply):

A. Manual
392 Responses

B. Electronic
241 Responses

Other
20 Responses

I do not know
25 Responses

N/A
38 Responses

25. Are the safeguards enforced?

Yes 401 Responses No 2 Responses I do not know 36 Responses N/A 44 Responses

26. Are the safeguards communicated throughout the Agency?

Yes 357 Responses No 48 Responses N/A 78 Responses

27. Does your agency educate employees (including temporary employees) on the personal information that is presently exempt from disclosure under the Open Public Records Act (OPRA)?

Yes **343 Responses** No **79 Responses** N/A **61 Responses**

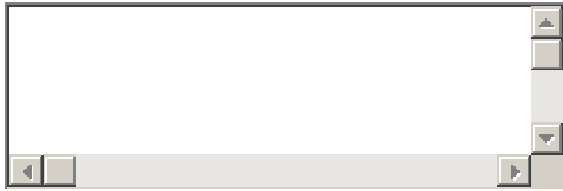
DATA DISSEMINATION AND DISCLOSURE TO THIRD PARTIES

(Please exclude disclosure of personal information your agency makes pursuant to OPRA requests when answering questions 28 thru 30.)

28. Does your agency share personal information with third parties outside of federal, state and local government?

Yes **133 Responses** No **275 Responses** I do not know **30 Responses** N/A **45 Responses**

29. If so, please name the third parties and describe what data and for what purpose:



See responses in separate report.

30. If so, does your agency obtain consent to share personal information with third parties (i.e. consent from your agency's upper management or the person to whom the information pertains)?

Yes **87 Responses** No **59 Responses** I do not know **36 Responses** N/A **301 Responses**

31. Does your agency sell, rent, or lease personal information?

Yes **6 Responses** No **399 Responses** I do not know **25 Responses** N/A **53 Responses**

32. If so, does your agency place restrictions on the subsequent use or dissemination of personal information by third parties?

Yes **33 Responses** No **20 Responses** I do not know **27 Responses** N/A **403 Responses**

APPENDIX B

Data Practices Survey Results: OTHER ANSWER CHOICES

PARTICIPANT INFORMATION

4. Who are the customers of your unit or agency?

Anyone (needing advise, referrals, or services) = 6

General motoring public = 1

Public employees and managers = 13

Grant recipients = 1

Job applicants = 1

Institutions of higher education = 1

Attorneys = 1

Permit applicants = 1

Those in need of police assistance = 2

Elderly = 1

Law enforcement agencies/community = 3

Community based organizations = 2

Healthcare providers and hospitals = 4

Prison inmates = 17

Criminal offenders = 1

State contractors = 1

Advocates = 1

Families = 1

Correctional institutions = 1

Parents and guardians of minor children = 1

Day care centers = 2

Non-profit organizations = 3

Patient need medical care = 1

Municipalities = 1

Toll payers = 1

Passengers = 1

Consular personnel = 1

Fire companies = 1

Casino licensees = 3

Homeless veterans = 1

Media = 1

Lottery players = 1

Investment bankers = 1

Genealogists = 1
Department licensees = 1
Financial institutions and other federal banking regulators = 1
Defendants = 1

DATA COLLECTION

1. Identify your agency's methods of collecting personal information from customers and other agency users:

Media = 1
Home sales = 1
Court documents = 3
Police departments = 1
FTP cite = 1
Classification face sheets = 1
CJIS background = 1
From other agencies = 11
Field inspections = 1
Interfaces = 1
Lawyer = 1
Subpoenas = 1
Inspections = 1
Computer inquiry = 1
Deeds = 1
Electronic tracking systems = 1
Net file transfer = 1
Virtual private network = 1

2. Identify the types of personal information your agency collects:

Drivers License = 5
ADA Accommodations = 1
Criminal, civil, and background histories/records = 13
Alcohol test results = 1
Pending discipline and litigation = 1
Workforce data = 1
Federal ID number = 3
Vital statistics for marriage, birth, and gender = 2
Death certificates = 1
Insurance information = 4
Information necessary to complete police investigations = 1
Medical records (doctor's office and school nurse's office) = 1
Vehicle registration numbers = 1
Method of payment = 1
Institutional telephone = 2

Tax ID number = 5
 Library materials that people borrow or reserve
 Vehicle identification numbers
 License plate numbers
 Medicaid information = 1
 Psychological information = 1
 Social security numbers = 1
 Information collected at another agency = 1
 Information required by regulation at inspection = 1
 INS information (country of origin)/citizenship information = 2
 Substance abuse profiles = 1
 State salary
 Personal financial statements/source of income/asset lists = 4
 Business telephone = 1
 Anonymous statistical information for the Affirmative Action Plan = 1
 Emergency contact information = 1
 Fire and medical training information = 1
 Information necessary for individual qualification verification (financial and other personal information)
 = 1
 Military information = 1
 Lease agreements = 1
 Minors' completed income tax returns and forms = 1
 Disability information = 1
 Utility account numbers = 1

3. Identify the source from which personal information is collected:

Medical practitioners = 3
 Background checks = 1
 Construction permit application = 2
 Field inspections = 1
 Businesses (third party contractors and vendors) = 9
 Investigative and incident reports = 3
 Orders to produce = 1
 District of residence = 1
 Private agencies = 1
 Current or former employers = 4
 S.S. death matches = 1
 Schools = 1
 Certifying boards = 1
 Application process = 1
 Credit reports = 1
 Insurers = 1
 Claims data = 1
 Deed = 1
 Educators and educational testing vendors = 2

Licensing files = 1
Casinos = 2
Attorneys = 1
Police = 1

5. What are the reasons that your agency collects personal information?

Enforce laws and regulations = 3
Issue licenses, permits, titles, and certificates = 8
Investigative purposes = 15
Recording and reporting purposes (including birth, death, medical and election records) = 20
Informational and analysis purposes = 3
Collections (including taxes and sales of lottery tickets) = 6
Verify proof of ownership = 2
Raffles and games of chance = 1
Respond to complaints = 3
Determine and administer escrow = 1
Employment purposes = 4
Payroll purposes = 3
Verify qualifications and/or eligibility (including financial status and moral character) = 14
Process applications = 2
Screening purposes = 2
Correspondence (including emergency contact, newsletter distribution and fundraising) = 6
Process OPRA requests = 2
Return repaired equipment (for inventory purposes) = 1
Grant processing = 1
School assignment = 1
Processing payments and claims = 7
Purchase order processing = 5
Mandated disclosure = 1
Human resource purposes = 1
Develop programs (including affirmative action plans) = 2
Security access purposes = 1
Verify relationship (including guardianship) = 2
Provide services or treatment (including medical care) = 8
Block inmate calls as requested by person to whom data pertains = 1
Classify inmates = 1
Motor vehicle assignment = 1
Education purposes = 1
Ticket and pass sales = 1
Issue replacement checks = 1
Structure project financing = 1
Dispute settlement and adjudicatory purposes = 1
Donations and grant making = 1
Training = 1
Registration = 2

Identify health coverage = 1
HMO rate setting = 1
Determining sanctions = 1
Vital Statistics = 1
Probate process = 1

DATA PROCESSING AND STORAGE

8. Data is processed:

By another state or local government agency = 25
By a federal government agency = 4
Computerized records = 1
Schedules, logbooks = 1
CRAF = 1
Statewide database = 1
State and federal requirements = 1
Custodian for loans = 1
Non-profit organization = 1
E-mail = 1

9. Data or records are stored:

By another state or local government agency = 66
By a federal government agency = 2
Computer files = 1
Educational testing service = 1
CRAF = 1
Non-profit organizations = 1

10. Disposal, destruction and shredding of records are done:

Both in-house and by an outside vendor = 1
By another state or local government agency = 27
By a federal government agency = 1
CRAF = 1
Records are not destroyed = 1
Non-profit organizations = 1

17. How is it determined whom within the agency handles personal information collected by the agency?

Case by case = 1
CJIS clearance = 1
System access restriction = 2

Committee = 1

Everyone within the agency handles personal information collected = 1

DATA USE

15. Indicate the purposes for which personal information is used by your agency:

Fire or medical reports/records = 3

Criminal or fire investigations or to verify complaints = 15

Payroll functions = 2

Tax collection = 1

Billing for services = 1

Benefits qualification = 3

Research program quality = 1

Documentation and record keeping = 2

Care, custody and rehabilitation of state prison inmates = 3

Classification of inmates = 4

OPRA requests = 3

Verification of license/credentials = 1

Educational assignments = 1

Payment and billing = 9

Expense reimbursement = 1

Purchase orders = 5

Emergency notification = 1

Veteran Entitlements = 1

Employment = 2

Processing permits, certifications and licenses = 6

Pre-qualification for bidding = 1

Analysis = 2

Security access to systems = 1

Plan service delivery = 1

Quality assurance = 1

Education services = 1

Motor vehicle assignment (motor pool forms) = 2

Legal reasons = 1

Tax purposes (including tax billing) = 4

Medical care = 2

Correspondence (mail out information and referrals) = 3

Vital statistics requests/demographic analysis = 2

Emergency contact = 3

Ticket and pass sales = 1

Enforcement of court orders = 1

Business qualification = 1

Finance projects = 2

Background checks = 1

Case work = 1

Fundraising, training and grant making = 2
Appeals and hearings processing = 2
Processing insurance claims and coverage = 3
Collect tolls = 1
Screening = 1
Customer assistance = 1
Processing sanctions = 1
FEMA reporting = 1
Use agreements = 1
Government programs = 1
Processing death certificates = 1
Laboratory testing = 1
Self exclusion program = 2
Appointment of fiduciary of estates = 1
Board appointments = 1
Collection of penalties = 1
Approval of officers/directors of financial institutions = 1
Record research = 1
Membership application = 1

DATA PROTECTION

24. If your agency protects personal information against risk of loss or unauthorized access, are the safeguards manual or electronic?

Both manual and electronic = 1
Locks on file cabinets = 3
Office is locked after business hours = 3
Computer system and database is locked and password protected = 4
Security card access = 2
Security officer monitors access = 1