

# THE PROTECTION OF PERSONAL INFORMATION IN INTERGOVERNMENTAL DATA-SHARING PROGRAMS

A Four-Part Report on Informational Privacy Issues in Intergovernmental Programs

June 30, 1998

Written by  
J. Keith Harmon  
Rae N. Cogar

---

Electronic Commerce, Law, and Information Policy Strategies



*A Program of the Ohio Supercomputer Center*

# THE PROTECTION OF PERSONAL INFORMATION IN INTERGOVERNMENTAL DATA-SHARING PROGRAMS

prepared for the

INTERGOVERNMENTAL ENTERPRISE PANEL  
c/o Office of Information Resources Management  
Department of Veterans Affairs  
Washington, District of Columbia  
<http://iep.fedworld.gov/>

by

J. Keith Harmon  
Rae N. Cogar

The Ohio Supercomputer Center, ECLIPS Program  
1224 Kinnear Road  
Columbus, Ohio 43212  
<http://www.osc.edu/eclips/>

June 30, 1998

This report was prepared for the ECLIPS program of the Ohio Supercomputer Center (OSC) with funding from the Intergovernmental Enterprise Panel (IEP). The views and opinions expressed by the authors are not necessarily those of ECLIPS, OSC, the IEP, the Ohio State University, or any other affiliated organization or institution.

# TABLE OF CONTENTS

<i>Table of Contents</i> .....	i
<i>Acknowledgements</i> .....	iii
<i>Executive Summary</i> .....	iv

## Part I

### THE LEGAL FRAMEWORK OF PRIVACY – THE FEDERAL SYSTEM

I.	Introduction .....	I-1
II.	Study Objectives .....	I-2
III.	The General Protections and Requirements of Federal Privacy Laws.....	I-4
	A.    What is Privacy? .....	I-4
	B.    Privacy, Confidentiality, and Security .....	I-5
	C.    The U.S. Constitution and Informational Privacy.....	I-5
	D.    Federal Statutory and Regulatory Protection .....	I-7
IV.	The Federal Privacy Infrastructure for Two Selected Federal Programs .....	I-16
	A.    The USDA Food Stamp Program's EBT Project .....	I-17
	B.    The HHS Child Support Enforcement Program's Federal Parent Locator Service/National Directory of New Hires .....	I-25

## Part II

### THE LEGAL FRAMEWORK OF PRIVACY – THE STATE AND LOCAL SYSTEMS

I.	Introduction to State Issues .....	II-1
II.	State Laws and Practices Related to Case Study Programs .....	II-1
	A.    Kansas .....	II-1
	B.    Maryland .....	II-6
	C.    Ohio .....	II-9
	D.    Texas .....	II-14
	E.    Washington .....	II-17
	F.    A Brief Look at Local and Tribal Issues.....	II-21

## Part III

### OBSERVATIONS AND DISCUSSIONS

I.	Introduction .....	III-1
II.	Observations and Discussions.....	III-1
	A.    Legal Issues .....	III-1

B.	Issues of Technology and Practice .....	III-5
C.	Speculative Issues .....	III-7

**PART IV:  
GUIDELINES FOR PROTECTING PRIVACY IN INTERGOVERNMENTAL  
PROGRAMS**

I.	Introduction .....	IV-1
II.	Some Proposed Guidelines .....	IV-1
	A. Defining the Data-Sharing Program .....	IV-1
	B. Considering the Role of Personal Information in the Program .....	IV-1
	C. Balancing Competing Interests .....	IV-2
	D. Designing the System .....	IV-2
	E. Constructing a Program-Specific Regulatory Framework for Privacy .....	IV-2
	F. Educating Participants and Data Subjects .....	IV-4
	G. Developing and Using a State Clearinghouse.....	IV-4
	H. Auditing and Overseeing Privacy Protection Practices .....	IV-4
	I. Planning for any Future Expansion of the Program.....	IV-4

**Appendix A – Selected Laws and Bibliography .....** A-1

I.	Books and Reports .....	A-1
II.	Law Review Articles.....	A-4
III.	Newsletters, Articles, Web Sites, and Other Information .....	A-4
IV.	Federal and State Statutes, Regulations, Circulars, and Executive Orders.....	A-9
	A. Federal Laws.....	A-9
	B. Federal Regulations .....	A-10
	C. OMB Circulars, Etc.....	A-10
	D. Executive Orders.....	A-11
	E. State Laws and Regulations.....	A-11
V.	Federal and State Case Law .....	A-12

**Appendix B – Project Team Information.....** B-1

## ACKNOWLEDGEMENTS

The authors would like to first thank the ECLIPS and Ohio Supercomputer Center staff for their invaluable help in researching and writing this study:

- Jeff Wilhelm and Matthew MacArthur were essential for their research on state and federal laws, Food Stamp and Child Support Enforcement practices, and other information needed to accomplish this study. In addition, we would like to thank them for their help in proofreading this paper and in preparing the bibliography.
- Cheryl Stevens provided a great deal of assistance by managing our contacts with state and federal officials. She also was invaluable in handling the operations end of this study.
- Dr. Steve Gordon, Deputy Director of the Ohio Supercomputer Center, provided much-needed guidance and advice throughout the course of this project.

We would also like to thank the state and federal officials who took time out of their busy schedules in order to provide us with critical information about the laws and practices surrounding the federal data-sharing programs. Without their cooperation, this study would have been much more difficult.

Finally, we would like to thank Professor George Trubow, Director of the John Marshall Law School Center for Information Technology & Privacy Law, for his advice on the complex issues of informational privacy.

# EXECUTIVE SUMMARY

## I. PURPOSE

Intergovernmental data sharing and information technology can help to make governments more efficient, by reducing the fraud, error, and costs associated with maintaining a segregated (and/or paper-based) system. However, there are recognized limits, as a matter of policy, that governments must consider before entering into any data-sharing program. One of these limits, and perhaps the one with the greatest potential to create public controversy, is the right of informational privacy. In addition, because of the great amount of variation among the ways that different jurisdictions protect privacy, privacy laws can act as *barriers* to intergovernmental data sharing.

To ensure that governments can reap the benefits of data sharing without unreasonably impinging on informational privacy rights or encountering legal barriers to interoperability with other jurisdictions, the Intergovernmental Enterprise Panel (IEP) commissioned ECLIPS, a program of the Ohio Supercomputer Center, to study the issues of informational privacy as they affect intergovernmental data sharing. The results of this study are set out in our full report, the *Protection of Personal Information in Intergovernmental Data-Sharing Programs*.

## II. SCOPE

Due to the fast-track nature of this study, ECLIPS has focused on the privacy laws and practices for two specific federal programs. Both programs are relatively new and are executed largely at the state level, with guidance and oversight by the federal government:

- The U.S. Department of Agriculture's Food Stamp/Electronic Benefits Transfer (EBT) program
- The U.S. Department of Health and Human Services' Federal Parent Locator Service/National Directory of New Hires

Most states are currently operating both of these programs, although at varying levels of progress. To limit the scope of this study, ECLIPS, in coordination with the IEP, has selected five states as the focus of our research. These states were chosen for their geographical diversity, as well as for the varied methods they use to execute each program:

- Kansas
- Maryland
- Ohio
- Texas
- Washington

The ECLIPS study of the privacy infrastructure for these two data-sharing programs is divided into four parts:

- Part One – The Legal Framework of Privacy: The Federal System
- Part Two – The Legal Framework of Privacy: The State and Local Systems
- Part Three – Observations and Discussions
- Part Four – Guidelines for Protecting Privacy in Intergovernmental Programs

### III. OBSERVATIONS

The following are summaries of some of the observations made in the full report. These observations are not meant to be conclusive, but they are an accurate reflection of what we learned from our research of the two programs and from our interviews with federal and state policy makers.

- At present, the Constitutional right to informational privacy, to the extent that it is recognized at all, has had little affect on government's collection and use of personal information.
- The Privacy Act does not always apply to data-sharing programs, particularly when the records are maintained by a state (even when the state is operating a *federal* program).
- Privacy protection at every level is a patchwork, with little in the way of a well-considered, integrated methodology for protecting personal information.
- The primary privacy protection for the case study programs comes from their respective federal program regulations, not from federal or state privacy laws.
- State laws cannot interfere directly with federal program regulations, but they can make interstate data sharing difficult. This is because states vary considerably in their treatment of privacy. For instance, if one state prevents a disclosure, while another does not, the ability for these states to share information may be limited.
- States are relying more and more on private contractors to operate data-sharing programs. Although a data-sharing program's privacy protections may not cover every conceivable use of personal information by a private contractor, the use of nondisclosure clauses by states in their contracts with private contractors is a good way to ensure the protection of privacy.

### IV . RECOMMENDATIONS

We recommend that federal policy makers consider the following steps to ensure that personal information is adequately protected before implementing any intergovernmental data-sharing program:

1. *Define the data-sharing program* carefully, to avoid encountering any unexpected privacy (or other) problems later. One focus here is to minimize the amount of personal information used to accomplish the goals of the program.
2. *Consider the role of personal information in the program.*
3. *Balance the competing interests* of achieving the program's primary purpose and protecting informational privacy (to the extent that these interests *are* in conflict).
4. *Design the system* to protect personal information.
5. *Construct a program-specific regulatory framework for privacy.*
6. *Educate participants and data subjects* about their respective responsibilities and rights under the law.
7. *Develop and use a state clearinghouse* to help states coordinate their differing legal, technical, and practical systems. This is especially important when data sharing will be among states, as well as with the federal government. True intergovernmental interoperability requires that different jurisdictions be aware of any existing conflicts so that they can work to overcome them.
8. *Audit and oversee privacy protection practices.*
9. *Plan for any future expansion of the program* with the protection of personal information in mind.

The full text of these "Guidelines for Protecting Privacy in Intergovernmental Programs" is set out in Part IV of our report, the *Protection of Personal Information in Intergovernmental Data-Sharing Programs*. These guidelines are not comprehensive, but they are a starting place where policy makers can begin to consider, in a systematic way, the protection of privacy as an integral component of any program that involves the sharing of personal information.

## PART I: THE LEGAL FRAMEWORK OF PRIVACY – THE FEDERAL SYSTEM

### I. INTRODUCTION

The growing use of information technologies to perform government functions has, with some irony, added an incredible amount of complexity to the process of governing. Limitations within the paper-based systems of the past that made information at least somewhat manageable are quickly disappearing. That manageability was, of course, often illusory--after all, the fact that information is manageable says nothing of the completeness, accuracy, or relevance of that information. Today, the improved controllability of information gained through the use of information technologies is often more than offset by the increased amount and complexity of the information at hand.

If dealing with larger amounts of information was the only problem, we could expect technology to offer new methods to help limit the problem. However, in addition to the greatly expanded size of databases, an additional issue arises: What are the rules and practices for handling the *sharing* of information among different agencies and levels of government?

Government, for a number of reasons, has a significant interest in sharing information on an intergovernmental scale. First, if different agencies collect similar information for similar purposes from the same person, then the collection process requires duplicative effort for the agencies, as well as for the person or entity providing the information. The ability of government agencies to share collections of information would help reduce that burden. Second, comparing information in different databases may help identify instances of fraud or error. For example, prisoner rolls have been matched against welfare records to prevent improper disbursement of certain welfare benefits to incarcerated--and therefore ineligible--individuals.

With widespread data sharing comes a host of new issues to settle. In order to get a handle on some of the most critical of these issues, the Intergovernmental Enterprise Panel<sup>1</sup> (IEP) has commissioned a number of studies<sup>2</sup> to identify existing and

---

<sup>1</sup>

The Intergovernmental Enterprise Panel (IEP) is an organization with representatives from Federal, State, and local governments. It emphasizes information technology solutions that will enable collaboration between all levels of government to improve intergovernmental service delivery to the public and increase the efficiency and effectiveness of government operations. The IEP was established by the Government Information Technology Service Board (GITSB) which is authorized by Executive Order 13011, Federal Information Technology.

*All About IEP: What is the Intergovernmental Enterprise Panel?* <<http://iep.fedworld.gov/about/>>.

potential problems in intergovernmental data sharing. The IEP has asked ECLIPS to research and report on the laws and practices for two separate areas: (1) the interoperability of systems across local, state, and federal agencies and (2) the protection of personal information held by and shared among all levels of government (this study).

The importance of dealing with potential problems in intergovernmental data sharing now, rather than later, cannot be overstated. Despite the problems that are arising due to the use of information technologies, governments are beginning to use these same technologies to make information *more* manageable and *more* useful. If issues such as interoperability and privacy can be properly addressed and dealt with, the full potential of data sharing can be met without unnecessary costs or the diminishment of personal privacy.

This paper takes a first look at the issue of how government-held personal information is protected--both in law and practice--for two specific federal programs as executed in five states. The next section provides some details about the study, including our scope and objectives.

## II. STUDY OBJECTIVES

The purpose of this study is to provide policy makers with a starting point for analyzing privacy issues in the planning and execution of intergovernmental data-sharing programs. Due to the fast-track nature of this study, ECLIPS has focused on the privacy laws and practices for two specific federal programs. Both programs are relatively new and are executed largely at the state level, with guidance and oversight by the federal government:

- The U.S. Department of Agriculture's Food Stamp/Electronic Benefits Transfer (EBT) program
- The U.S. Department of Health and Human Services' Federal Parent Locator Service/National Directory of New Hires

Most states are currently operating both of these programs, although at varying levels of progress. To limit the scope of this study, ECLIPS, in coordination with the IEP, has selected five states as the focus of our research. These states were chosen for their geographical diversity, as well as for the varied methods they use to execute each program:

---

<sup>2</sup> See generally Harvard University John F. Kennedy School of Government, *Standing in the Way of Tomorrow: The Federal View of Barriers to Intergovernmental IT Initiatives* <<http://iep.fedworld.gov/library/harvard1.html>>; Public Technology, Inc., *Intergovernmental Enterprise Report Phase I* <<http://iep.fedworld.gov/library/phase1.html>>; Public Technology, Inc., *Intergovernmental Enterprise Report Phase II* <<http://iep.fedworld.gov/library/phase2.html>>; National Governors' Association, *Task One Report: Barriers to Intergovernmental Enterprise* <<http://iep.fedworld.gov/library/task1.html>>; National Governors' Association, *Task Two and Three Report: Best Practices and Recommendations for IEP Demonstrations* <<http://iep.fedworld.gov/library/task2.html>>.

- Kansas
- Maryland
- Ohio
- Texas
- Washington

The ECLIPS study of the privacy infrastructure for these two data-sharing programs is divided into four parts. Each part of the study is identified below, with a brief description of our objectives.

#### Part One – The Legal Framework of Privacy – The Federal System

- The objective of the federal study is to identify the principal federal laws and regulations protecting informational privacy, including program-specific and more general rules. This study also sets out the general guidelines for executing the programs, as described in each program's regulations.

#### Part Two – The Legal Framework of Privacy – The State and Local Systems

- The state and local study identifies state laws and regulations that apply or may apply to the selected federal programs. Although these laws are unlikely to interfere with the data-sharing components of the federal programs, some states may provide *additional* protections for privacy that are not required by federal law. We will also identify variances in the design of the programs among the states to the extent that those variances affect privacy.

#### Part Three – Observations and Discussions

- In this part of the report, ECLIPS takes the lessons learned from the federal and state research and uses them to address several issues:
  - Whether, and to what degree, privacy laws *by their terms* limit intergovernmental electronic data-sharing programs. This question also encompasses any variation in how each state protects privacy.
  - Whether, and to what degree, compliance with privacy laws *in practice* limits intergovernmental electronic data-sharing programs.
  - Whether, and to what extent, the level of individual privacy protection *expected by data subjects* is accommodated or affected by intergovernmental electronic data-sharing programs.

#### Part Four – Guidelines for Protecting Privacy in Intergovernmental Programs

- This part of our study is intended to serve as a tool that policy makers can use when considering future intergovernmental data-sharing programs.

### III. THE GENERAL PROTECTIONS AND REQUIREMENTS OF FEDERAL PRIVACY LAWS

#### A. WHAT IS PRIVACY?

Most people--judges and legislators included--define privacy much like Justice Stewart defined obscenity: "I know it when I see it. . . ."<sup>3</sup> The result of this approach has been that privacy laws are usually created on an ad hoc basis, with no clear unifying principle holding the laws together. Most "rights" recognized today have a fairly substantial foundation in the Constitution, in common law, or in both. However, privacy, as a freestanding right, has an independent foundation in neither. In fact, the legal protection of privacy is a recent practice, with the most significant protections evolving only during the past thirty years or so. This latecomer status does not mean that privacy is not an important right--far from it. While privacy may be an uncertain and loosely protected right, there is little doubt that it is an increasingly important one to the public at large.

Today, privacy shows up in a myriad of ways throughout the legal system. The range of what is called a "privacy interest" is quite broad--from the quasi-property right of the Fourth Amendment's protections against unreasonable searches and seizures to the "freedom to make important decisions" found in several cases involving family rights. Yet in virtually every kind of privacy-related law, there are common questions: What do we as a society expect to be private? To what degree is the government (or others) prevented from invading that privacy? Without a clear definition of privacy, these questions are difficult to answer.

Rather than attempt to define what privacy means as a general concept, we will reduce the scope of our definition to a particular kind of privacy--to what is known as "informational privacy". Most of the debate over this kind of privacy is not over its definition; instead, the debate hinges on the extent to which this interest should be protected. Preferring the straightforward definition for this study, we define informational privacy as "the interest in the collection, maintenance, use, and dissemination of personal information".<sup>4</sup> Clearly, this interest, which is not considered an absolute one, waxes and wanes depending on the purpose for the information collection/use and the identity of the party collecting/using the information.

In this study, we focus on informational privacy only as it concerns *government* collections and uses of personal information. As an aside, it is important to note that informational privacy is not merely an interest in what government does with personal information, it is really an interest in what *any* party does with personal information. However, the issues are different when the government is the collector or user of personal information. As with many government activities, the rights of an individual must be weighed against the interests of society at large. With informational privacy,

---

<sup>3</sup> *Jacobellis v. Ohio*, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

<sup>4</sup> GEORGE TRUBOW, *WATCHING THE WATCHERS: THE COORDINATION OF FEDERAL PRIVACY POLICY*, Benton Foundation Project on Communications and Information Policy Options 5 (1989).

the interest is still uncertain enough to make this balancing process difficult, particularly if the importance of informational privacy is not widely understood.

This study does not attempt to say to what degree informational privacy should be recognized; rather, it is an attempt to identify the degree to which informational privacy *is* recognized by federal and state law.

## B. PRIVACY, CONFIDENTIALITY, AND SECURITY

This study does not consider the issues of computer security except to the extent that such issues are inseparable from privacy issues. This may strike some readers as counterintuitive--aren't security and privacy really the same thing? In fact, they are not. Security is a *method* for protecting information, while privacy is a *reason* for protecting information. For example, an agency might want to keep information confidential<sup>5</sup>--perhaps because the information is a trade secret or implicates national security. The interests in protecting a trade secret or national security are usually unrelated to the interests in protecting the privacy of an individual. This is not to suggest that security is unrelated to privacy; in fact, the security of a system plays a major role in preventing unreasonable disclosures of information.

However, even in this preliminary study, it has become apparent that one of the problems with privacy policy is that a number of policy makers and officials make the mistake of assuming that system security equals privacy protection. It is a mistake to make this assumption because the protection of privacy is an end in itself, while system security is only a means for reaching that end. To determine how strong security must be or what should be done when security is breached, a policy maker must first consider the interest that motivates the use of security measures in the first place.

This study does not answer the question of whether this fallacy has the potential to undermine the importance and the practical application of the legal protection of personal information; however, it does assume that, as a matter of policy, the issues of privacy, confidentiality, and security should be considered at least somewhat independently. This viewpoint is reflected in the fourth part of this study, *Guidelines for Protecting Privacy in Intergovernmental Programs*.<sup>6</sup>

## C. THE U.S. CONSTITUTION AND INFORMATIONAL PRIVACY

The starting place for analyzing any issue involving individual rights is the U.S. Constitution. Usually, when the Constitution explicitly deals with an individual right, it expresses that right in terms of limits placed on government. That is, despite a public perception that the Bill of Rights is a *grant* of rights to the people, the Constitution

---

<sup>5</sup> Confidentiality can also be distinguished from privacy: "Confidentiality is a characteristic of information management and implies that information can be disclosed only to certain persons under specified circumstances". U.S. DEPT. OF AGRIC., EBT DATA PRIVACY ISSUES FOR FOOD BENEFIT PROGRAMS 2 (Aug. 1994).

<sup>6</sup> See *infra* Part IV.

actually reflects an Enlightenment view of the world--that there are natural rights inherent in human existence that are beyond the caprice of government. Thus, the Bill of Rights tells us what the government *cannot* do, not what the people *can* do.<sup>7</sup>

The importance of this rule of Constitutional interpretation is that the focus of any analysis of individual rights must be on the government. What is the government doing? How do its actions impinge on a right? Yet before asking even these questions, there is another question that must be answered: Is the "right" actually one protected by the Constitution?

With some rights, this analysis is not necessary. For instance, the freedom of speech is expressly protected in the Constitution--there is no question that it is a "right". However, there are some other areas that are not so clear. One of these is informational privacy.

*Whalen v. Roe*<sup>8</sup> was the first time the Supreme Court addressed the possible existence of a Constitutionally protected right of informational privacy that applies when government collects personal information. Although delving too deeply into the details of this case and its progeny would be counterproductive here, there are a few points about *Whalen* that are worth a brief look.

*Whalen* dealt with a New York law requiring doctors to disclose to the state personal data about patients receiving certain kinds of prescriptions. When considering whether there was a right to informational privacy that was being impinged upon by this law, the Court found that "[t]he cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions."<sup>9</sup>

The Court recognized that the New York statute could threaten these interests but found that the state had taken appropriate measures to protect the interests in the wording and execution of the law. However, the Court did leave open the possibility that the collection and disclosure of personal information by the government *could* be unconstitutional in certain, unspecified situations:

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of

---

<sup>7</sup> Consider the First Amendment: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press. . .". U.S. CONST. amend I. This does not grant a right to citizens to speak; it limits the ability of the government to interfere with that right.

<sup>8</sup> 429 U.S. 589 (1977).

<sup>9</sup> *Id.* at 598-600 (footnotes omitted).

the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data--whether intentional or unintentional--or by a system that did not contain comparable security provisions.<sup>10</sup>

For our purposes, the interests recognized in *Whalen* should not affect the execution of data-sharing programs that are covered by the Privacy Act or a state equivalent, or that have other protections against "unreasonable" disclosures. However, all levels of government must take care to prevent these "unwarranted disclosure(s) of accumulated private data". Courts have already found and will continue to find, in certain limited situations, that the state's interest in collecting and disclosing personal information can be outweighed by the individual's Constitutional right to informational privacy.<sup>11</sup> As information technology allows personal information to be more and more exposed to the purview of unintended parties, this right may be expanded--either by the courts or by legislatures.

#### D. FEDERAL STATUTORY AND REGULATORY PROTECTION

##### 1. *The Privacy Act of 1974*<sup>12</sup>

The lack of a clearly defined Constitutional basis for informational privacy does not mean that there are no limitations on disclosures of personal information. In fact, Congress dealt with this issue twenty-five years ago in the Privacy Act of 1974.<sup>13</sup>

The Privacy Act, like a number of privacy laws and regulations, came about as the result of a specific instance of misconduct. The driving force behind the passage of the Privacy Act was no less than the public outcry against the many invasions of privacy that occurred during the Watergate scandal. Because this concern was focused on the

---

<sup>10</sup> *Id.* at 605-06 (footnotes omitted).

<sup>11</sup> See generally *Doe v. Borough of Barrington*, 729 F. Supp. 376 (D.N.J. 1990) (holding that a police officer's disclosure of an individual's HIV status to a neighbor of the individual served no state interest); *Hodge v. Carroll County Department of Social Services*, 812 F. Supp. 593 (D.Md. 1992) (noting that the *Whalen* interest in "avoiding disclosure of personal matters" encompassed familial privacy).

<sup>12</sup> This discussion of the Privacy Act is limited to the plain language of the Act, the OMB Guidelines, and the case law, insofar as the various courts are in agreement. In the next part of this study, when we focus on the execution of the case study programs in five selected states, these variations may become more important.

<sup>13</sup> 5 U.S.C. § 552a (1997).

government's collection and disclosure of personal information, Congress drafted the Privacy Act to specifically limit what the federal government--not the states or the private sector--could do with personal information.

The Privacy Act states that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains. . .".<sup>14</sup> This is the basic principle of the Privacy Act--that no record be disclosed without the permission of the individual who is the subject of that record. Yet, as with many laws, the definitions of the terms used and the exceptions to the law's restrictive language are what truly define the scope of the Privacy Act. In particular, we will look at the limitations of the general protection of the Act insofar as an individual's information qualifies as a record in a system of records, and we will examine the extensive exemptions to the Act's non-disclosure requirement. We will also review the issues of computer matching, and we will briefly examine who oversees the proper execution of the Privacy Act.

a. *What kind of information is protected by the Privacy Act?*

The Privacy Act limits an *agency's* disclosure of the *records of individuals* that it *maintains* in a *system of records*. The Act defines the italicized terms, and it is useful to include those definitions here:

<b>Agency</b>	"[I]ncludes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." <sup>15</sup>
---------------	--

---

<sup>14</sup> 5 U.S.C. § 552a(b).

<sup>15</sup> 5 U.S.C. § 552(f)(1) (1997). This definition is incorporated by reference; the actual text in the Privacy Act reads, "the term 'agency' means agency as defined in section 552 [(f)](e) of this title". 5 U.S.C. § 552a(a)(1).

<b>Record</b>	"[A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual." <sup>16</sup>
<b>Individual</b>	"[M]eans a citizen of the United States or an alien lawfully admitted for permanent residence." <sup>17</sup>
<b>Maintain</b>	This term "includes maintain, collect, use, or disseminate". <sup>18</sup>
<b>System of Records</b>	"[A] group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." <sup>19</sup>

However, an analysis of what kind of information the Privacy Act actually protects requires expanding on these statutory definitions and answering the following question: When, not counting any exemptions or exceptions, will an agency be prevented from making a disclosure (without the permission of the individual) under the Privacy Act? The answer to this question is actually fairly simple, although it is not necessarily clear from a reading of the Act. Therefore, a second look at the practical meaning of some of the terms set out above is in order.

### Individual

- The information in question must be about an individual. The Privacy Act is intended to protect personal information, not information about companies, organizations, or government agencies. This is in contrast to a number of other rights that *both* individuals and organizations might have, such as the freedom of speech, the right to own and transfer property, et cetera. Therefore,

**The first question a policy maker should ask when dealing with a Privacy Act issue is whether the information in question is about an individual. If the information is not about an individual, then the Privacy Act does not apply.**

<sup>16</sup> 5 U.S.C. § 552a(a)(4).

<sup>17</sup> 5 U.S.C. § 552a(a)(2).

<sup>18</sup> 5 U.S.C. § 552a(a)(3).

<sup>19</sup> 5 U.S.C. § 552a(a)(5).

## Record

- The definition of a record in the Privacy Act and as interpreted by the case law clearly shows that this is not a limiting characteristic of the Act. Instead, a record is virtually any kind of information kept about an individual that contains that individual's name or some other personal identifier.

## System of Records

- The requirement that the record be maintained in a system of records is often a stumbling block to understanding for people who encounter Privacy Act issues. The reason for this is the additional requirements imposed by the courts. In essence, an agency only keeps a "system" of records when the records are retrievable by name or personal identifier *and* are actually retrieved by name or personal identifier. Although many records maintained by agencies easily meet these criteria, it is important to understand that if both of these elements are not met, then the Privacy Act does not apply. Therefore,

**The second question a policy maker should ask when dealing with a Privacy Act issue is whether the information in a record includes a name or other personal identifier *and* whether the agency actually retrieves the record by name or personal identifier. If *both* elements are not present, then the Privacy Act does not apply.**

### *b. Who is regulated by the Privacy Act?*

"The Privacy Act of 1974 regulates the collection, use, and disclosure of personal information by federal agencies and is the principal means of privacy protection in the Federal realm. It does not apply to information collection efforts or systems funded with Federal money if the information is controlled by State or local governments."<sup>20</sup>

This statement is consistent with the plain meaning of the Privacy Act's definition of "agency" as a federal entity but adds the additional meaning that an "agency" is not a state entity, even if the state program is a federally-initiated or federally-funded program. This definition also makes it clear that the Privacy Act has no bearing on the actions of the private sector.<sup>21</sup> Therefore,

**The third question a policy maker should ask when dealing with a Privacy Act issue is whether the "agency" maintaining a system of records is a federal agency. If not, the Privacy Act does not apply.**

<sup>20</sup> U.S. DEPT. OF AGRICULTURE, FOOD AND NUTRITION SERVICE, EBT DATA PRIVACY ISSUES FOR FOOD BENEFIT PROGRAMS, Appendix I, A-1 (Aug. 1994).

<sup>21</sup> See *infra* note 74 and the accompanying text for a discussion of the Federal Acquisition Regulations.

c. *What are the protections of the Privacy Act?*<sup>22</sup>

The Privacy Act assigns a number of duties to agencies maintaining a system of records.<sup>23</sup> These duties are intended to maximize the transparency, accuracy, and security of personal information held by government. In addition, these responsibilities are imposed on agencies to minimize the impact of government data collection activities on individuals. To this end, agencies are responsible for--

- Maintaining only information that is "relevant and necessary" to the agency's mission<sup>24</sup>
- Collecting information directly from the individual to the greatest extent practicable<sup>25</sup>
- Informing data subjects of--
  - The authority and principal purpose of the data collection
  - Whether the data subject's participation in the collection is mandatory or voluntary
  - The routine uses of that information that may occur
  - The repercussions facing the data subject if he does not provide the information

Agencies are also responsible for publishing "a notice of the existence and character of the system of records", maintaining accurate records, and keeping the records secure. Violation of any of these requirements can result in civil or criminal liability.<sup>26</sup>

d. *When and how can an agency disclose information to a third party?*

There are three principal situations when an agency may disclose information that it maintains in a system of records:<sup>27</sup>

Situation 1: The data subject provides written permission for the disclosure.

- This, of course, is the simplest situation. So long as the data subject has authorized a particular disclosure, there can be no violation of the Privacy Act when the agency makes that authorized disclosure.

---

<sup>22</sup> There are several protections, such as agency accounting requirements, that are not discussed here. This section deals with only the major protections.

<sup>23</sup> See 5 U.S.C. § 552a(e)(1)-(12) for a complete list of agency requirements under the Privacy Act.

<sup>24</sup> 5 U.S.C. § 552a(e)(1).

<sup>25</sup> 5 U.S.C. § 552a(e)(2).

<sup>26</sup> 5 U.S.C. § 552a(g) and (i).

<sup>27</sup> Note that if the information is not held by an "agency"--a federal entity--and it is not in a "system of records", then the Privacy Act does not apply at all, and the entity holding the information may disclose it freely (unless other laws or regulations apply). Of course, as discussed above, there may be some restrictions imposed by the limited information privacy protections found in the U.S. Constitution. Also, if the "agency" in question is a state agency, then the state's constitution or laws may limit disclosures as well.

Situation 2: The Privacy Act's exceptions to the written permission requirement apply.

- There are twelve forms of disclosure that do not require the written permission of the data subject.<sup>28</sup> Most of these are fairly rare and will not occur often in intergovernmental data-sharing activities or are not really disclosures at all.<sup>29</sup> However, one of these exceptions is very significant and is the principal manner in which agencies make disclosures. This is the "routine use" exception.
- Routine uses are disclosures by the agency for purposes that are "compatible with the purpose for which [the information] was collected".<sup>30</sup> A common example of a routine use is when a federal agency collects information for a purpose, say for administration of a federal benefits program, and discloses that information to a state agency that operates a parallel benefits program. This disclosure can be made without the written permission of the data subject but must be done in a prescribed manner:
  - (1) *Compatibility of the use.* The routine use must be "compatible with the purpose for which [the information] was collected".<sup>31</sup>
  - (2) *Notice in the Federal Register.* The agency must provide notice for all routine uses by publishing required information about each use in the Federal Register.
  - (3) *Actual notice.* The agency must provide actual notice of the routine use to the data subject.<sup>32</sup>
- Although beyond the scope of this section of our study, it is worth noting that the routine use exception is by far the dominant means through which personal information flows from and among government agencies. In fact, a number of critics argue that routine uses are *too* routine, that agencies simply call any possible use a routine use without really complying with the compatibility requirement.<sup>33</sup> To the extent that this is or is not true with our case studies, we will focus on this issue in our analysis of the states' actual practices in Part II of this study. For now, it is sufficient to note that routine uses are a major component of Privacy Act activities.

---

<sup>28</sup> 5 U.S.C. § 552a(b)(1)-(12).

<sup>29</sup> Assuming a reasonable amount of security is maintained, internal "disclosures" and disclosures made for statistical purposes should not threaten the privacy of the data subject--in the former case, the information is not leaving the agency authorized to use the information. In the latter instance, the nature of the disclosure is such that the personal identifier is stripped, therefore eliminating the "personal" nature of the information. The law enforcement and court order exceptions are disclosures in the full meaning of the word, but are not routine and are limited in nature.

<sup>30</sup> 5 U.S.C. § 552a(a)(7).

<sup>31</sup> *Id.*

<sup>32</sup> This requirement is not found in the language of the Privacy Act; rather, it has been interpreted as a necessary part of the Act by the courts. *U.S. Postal Service v. National Ass'n of Letter Carriers*, 9 F.3d 138, 146 (D.C. Cir. 1993); *Covert v. Harrington*, 876 F.2d 751, 755-56 (9th Cir. 1989).

<sup>33</sup> PAUL M. SCHWARTZ & JOEL R. REIDENBERG, *DATA PRIVACY LAW* 97 (1996); see generally Todd Roberts Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U.L. REV. (1991).

Situation 3: The disclosure in question is one that is exempted by the Privacy Act.

- The Privacy Act sets out general and specific exemptions that give an agency some leeway in making certain kinds of disclosures.<sup>34</sup> None of these exemptions allows an agency to evade the basic requirements of the Privacy Act; however, they do allow the agency to limit some of its responsibilities, as discussed under section *III.D.1.c.* above.

e. *What about computer matching? What is it, and when can it occur?*

Computer matching, more accurately called data matching, "is the electronic comparison of two or more sets of records in order to find individuals in more than one database".<sup>35</sup> Although the government has been involved in computer matching for some time, it was not until the late 1980s that Congress paid particular attention to the practice. Concerned that computer matching was permitting agencies to evade the protections of the Privacy Act,<sup>36</sup> Congress passed the Computer Matching and Privacy Protection Act of 1988<sup>37</sup> and the Computer Matching and Privacy Protection Amendments of 1990.<sup>38</sup> These laws amended the Privacy Act to take into account the practice of computer matching and to establish procedures for computer matches made by and among government agencies.

As a practical matter, the amendments do not create any substantive privacy protections; instead, they set out procedural requirements for agencies that engage in computer matching. Therefore, these requirements are relevant to this study only to the extent that they create additional responsibilities/burdens for entities involved in computer matching. These procedural requirements are broken down into two classes: (1) pre-match ("matching agreements") and (2) post-match ("verification and opportunity to contest findings").

### Matching agreements<sup>39</sup>

- Matching agreements are contracts between the source and recipient agencies in a data-sharing program. They set out the purpose, justification, and procedures for the intended matching program. Although the Privacy Act does not establish criteria for determining when matching is appropriate, these agreements are important because they provide notice and regulate the behavior of each party to the match. Matching agreements are mandatory for any

---

<sup>34</sup> 5 U.S.C. § 552a(j) and (k).

<sup>35</sup> See SCHWARTZ & REIDENBERG *supra* note 33, at 100-01.

<sup>36</sup> The problem was that every computer match was being treated as a routine use. By automatically equating computer matching to routine use, agencies avoided the consent and compatible use requirements at the core of the Privacy Act.

<sup>37</sup> Pub. L. No. 100-503, 102 Stat. 507 (codified as amended at 5 U.S.C. § 552a).

<sup>38</sup> Pub. L. No. 101-508, 104 Stat. 3388 (codified as amended at 5 U.S.C. § 552a).

<sup>39</sup> 5 U.S.C. § 552a(o).

computer matching program.

### Verification and opportunity to contest findings<sup>40</sup>

- This provision of the Privacy Act is concerned with due process issues-- specifically when a computer match may affect a data subject's rights under a federal benefits program. Before taking any adverse action against the data subject based on a computer match, the agency must independently verify the information<sup>41</sup> and allow the data subject an opportunity to contest the findings.<sup>42</sup>

The Computer Matching Act also added some oversight provisions to the Privacy Act. These are briefly discussed in the next section.

#### *f. Who oversees compliance with the Privacy Act?*

- 1) Data Integrity Boards.<sup>43</sup> Data Integrity Boards are required for agencies that are involved in computer matching activities. These boards are composed of senior agency officials and have the responsibility of reviewing matching agreements and programs for compliance with federal privacy laws. Data Integrity Boards also serve a clearinghouse and reporting function.
- 2) Office of Management and Budget.<sup>44</sup> The Privacy Act creates a very broad oversight role for OMB. First, OMB is required to issue guidelines that agencies may use to interpret the provisions of the Privacy Act.<sup>45</sup> Second, OMB provides "continuing assistance to and oversight of the implementation of [the Privacy Act] by agencies".<sup>46</sup> Finally, OMB is responsible for overseeing the actions of each agency's Data Integrity Board.<sup>47</sup>
- 3) Congress. There are several reports that must be provided regularly to Congress under the Privacy Act. The purpose of these reports is to keep Congress informed of the kinds of data-sharing activities in which federal agencies are involved.

---

<sup>40</sup> 5 U.S.C. § 552a(p).

<sup>41</sup> 5 U.S.C. § 552a(p)(1)(A). This requirement is not necessary if "the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program" and there is a "high degree of confidence that the information. . . is accurate". 5 U.S.C. § 552a(p)(1)(A)(ii).

<sup>42</sup> 5 U.S.C. § 552a(p)(1)(B).

<sup>43</sup> 5 U.S.C. § 552a(u). Aside from a Data Integrity Board, each agency has what is known as a Privacy Act officer. This position is not required by the Privacy Act but is a mid-level official responsible for many of the day-to-day paperwork requirements of the Privacy Act. Such officials are necessary, since Data Integrity Boards are involved only at the highest level.

<sup>44</sup> 5 U.S.C. § 552a(v).

<sup>45</sup> 5 U.S.C. § 552a(v)(1). See *also* the OMB Guidelines to the Privacy Act as set out in 40 Fed. Reg. 28, 948-78 (1975); 40 Fed. Reg. 56, 741-43 (1975); 48 Fed. Reg. 15, 556-60 (1983); 52 Fed. Reg. 12, 990-93 (1987); 54 Fed. Reg. 25, 818-29 (1989); 56 Fed. Reg. 18, 599-601 (proposed Apr. 23, 1989); 61 Fed. Reg. 6, 428, 6, 435-39 (1996).

<sup>46</sup> 5 U.S.C. § 552a(v)(2).

<sup>47</sup> 5 U.S.C. § 552a(u).

2. *Individual access to records under the Privacy Act and the Freedom of Information Act privacy exemptions*

a. *Access under the Privacy Act*

The Privacy Act provides another safeguard by allowing a data subject to access and amend records concerning him.<sup>48</sup> The "Access to Records" section of the Act sets out procedures for a data subject's access to his records and also provides rules for agencies to follow in deciding whether to amend a data subject's record.

b. *Access under the Freedom of Information Act*<sup>49</sup>

In many ways, the policies behind the Freedom of Information Act (FOIA) appear to be in stark opposition to those behind the Privacy Act. The Privacy Act exists to limit the ability of government to disclose certain kinds of information. The FOIA exists to limit the ability of government to *refuse* to disclose certain kinds of information. However, these laws, despite appearances otherwise, are not contradictory. The FOIA requires government agencies to disclose most of the information that they hold, but the FOIA also provides for certain exemptions that allow an agency to refuse a requested disclosure.

Among the exemptions to the FOIA are two that are intended to protect privacy.<sup>50</sup> However, it is important to realize that if the FOIA mandates disclosure of a record and the FOIA privacy exemptions do not apply, the Privacy Act, by its own terms, cannot interfere with that disclosure.<sup>51</sup>

For government programs that involve data sharing, the important point to note is that the FOIA can, in very limited circumstances,<sup>52</sup> override the protections of the

---

<sup>48</sup> 5 U.S.C. § 552a(d).

<sup>49</sup> 5 U.S.C. § 552 (1997).

<sup>50</sup> Exemptions 6 and 7(c) are the "privacy exemptions" to the FOIA:

This section does not apply to matters that are . . . (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy. . . [and] (7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information. . . (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy.

5 U.S.C. § 552(b)(6) and (7)(C).

<sup>51</sup> 5 U.S.C. § 552a(b)(2).

<sup>52</sup> See *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1985). The Court found that the FOIA's "central purpose is to ensure that the Government's activities be opened to the sharp eye of public scrutiny, not that information about private citizens that happens to be in the warehouse of the Government be so disclosed". *Id.* at 774. In fact, the Court noted that "in none of our cases construing the FOIA have we found it appropriate to order a Government agency to honor a FOIA request for information about a particular private citizen." *Id.* at 774, 775.

Privacy Act. Furthermore, data subjects can use FOIA to get access to records that are exempted from the individual access provisions of the Privacy Act.<sup>53</sup>

### 3. *Other protections and requirements*

There is one fundamental truth about information privacy law in the United States--it is a patchwork. At every level of government, protection of informational privacy tends to evolve from specific instances that "shock the consciousness". As discussed earlier in this report, the Privacy Act was largely the result of the national outcry about the misuse of personal records by the Nixon Administration. Congress passed the Video Privacy Protection Act of 1988<sup>54</sup> in response to the concerns raised when Supreme Court nominee Robert Bork's video rental records were obtained during his confirmation hearings. A number of other laws have been passed dealing with specific kinds of records or specific industries.<sup>55</sup>

For the most part, the Privacy Act, state equivalents to the Privacy Act, the programs' enabling laws and regulations, and a variety of contract provisions will govern intergovernmental data-sharing programs.<sup>56</sup> On occasion, depending on the type of information shared and who is disclosing or receiving the information, other laws may apply. For example, the Tax Reform Act of 1976<sup>57</sup> and the Right to Financial Privacy Act of 1978<sup>58</sup> may apply in certain circumstances.

## IV. THE FEDERAL PRIVACY INFRASTRUCTURE FOR TWO SELECTED FEDERAL PROGRAMS

Although the Privacy Act establishes general limitations on what government can do with personal information, it is difficult, if not impossible, to discuss the overall protections afforded to informational privacy without looking at them in context. The type of information being protected, the planned uses of that information, and the extent to which that information will be disclosed are all relevant to the discussion, as are a number of other factors.

In addition, the Privacy Act, though a starting place for any analysis of informational privacy at the federal level, is usually not the *primary* source of protection in any given government program that uses personal information. Congress has, when

---

<sup>53</sup> See DEPT. OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974 638-647 (1997) for a discussion of the relationship between the Privacy Act and FOIA when a data subject requests a record on himself.

<sup>54</sup> 18 U.S.C. § 2710.

<sup>55</sup> For example, see the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 (prohibiting the unauthorized interception of communications or transmissions); the Fair Credit Reporting Act, 15 U.S.C. § 1681 (imposing limits on disclosures made by consumer reporting agencies); and the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (requiring states to protect student records as a condition to federal funding).

<sup>56</sup> The use of contracts among the states, federal agencies, and the private sector will be covered in our review of state laws and practices. See *infra* Part II.

<sup>57</sup> 26 U.S.C. § 6103 (providing privacy protection for tax return information).

<sup>58</sup> 12 U.S.C. § 3401 (places limits on government access to customer information held by financial institutions).

it has spoken to the issue at all, incorporated specific privacy protections into the enabling legislation for federal programs.

Because of the need to look at informational privacy as it is applied in specific programs, we have selected two programs on which to focus--the USDA Food Stamp Program's EBT project and the HHS Child Support Enforcement Program's Federal Parent Locator Service/National Directory of New Hires project.

#### A. THE USDA FOOD STAMP PROGRAM'S EBT PROJECT

##### 1. *Program description*

In 1984,<sup>59</sup> the U.S. Department of Agriculture (USDA) began testing the possible use of electronic benefits transfer (EBT) systems to deliver food stamps. This program has expanded over the years, with accelerated activity in recent years due to the impetus of the National Performance Review and the Personal Responsibility and Work Opportunity Reconciliation Act of 1996.<sup>60</sup>

The USDA's regulations on the use of EBT set out a basic description of the program:

An on-line EBT system is a computer-based system in which the benefit authorization is received from a central computer through a point-of-sale (POS) terminal. Eligible households utilize magnetic-stripe plastic cards and have accounts maintained at the central computer in lieu of food stamp coupons to purchase food items at authorized food retailers. Once certified, the household's benefits are electronically loaded into a central computer account for each month during the certification period. Checkout lanes at authorized food retailers are to be equipped with POS terminals. When the transaction occurs, the POS terminals connect on-line to the central computer database; verify the validity of the Personal Identification Number (PIN), card number, and the amount of available benefits in an EBT account; obtain authorization for each purchase and initiate the debiting of the household's account and the crediting of the retailer's account.<sup>61</sup>

As is true with the Food Stamp Program in general, the operation of these EBT programs is conducted principally by state agencies. The USDA is largely involved only

---

<sup>59</sup> Oversight of the Implementation of the Electronic Benefit Transfer System for the Food Stamp Program: Before the Subcomm. on Departmental Operations, Nutrition, and Foreign Agriculture of the House Committee on Agriculture (Mar. 12, 1997)

<[http://commdocs.house.gov/committees/ag/hagebt.000/hagebt\\_of.htm](http://commdocs.house.gov/committees/ag/hagebt.000/hagebt_of.htm)>.

<sup>60</sup> 7 U.S.C. 2016(i)(1)(A): "Not later than October 1, 2002, each State agency shall implement an electronic benefit transfer system under which household benefits. . .are issued from and stored in a central databank, unless the Secretary provides a waiver for a State agency that faces unusual barriers to implementing an electronic benefit transfer system."

<sup>61</sup> 7 C.F.R. § 274.12(a) (1998).

to the extent of setting guidelines and auditing program performance. Thus, defining the precise approach that every state takes in implementing and operating its EBT program is difficult without analyzing the laws and the prevailing practices of each state.<sup>62</sup> However, there are common factors among the state programs that can be discussed, including the data shared, the entities that supply or use that data, and the application of federal laws to the data sharing.

## 2. Data elements

There are several major times when data will be collected, including when the prospective food stamp client submits an application, when an EBT transaction occurs, and when a state or federal agency audits or investigates EBT activities. Due to the fact that most of the initial information is collected by the states, the specific data elements may vary from program to program. Also, the different points of collection may involve different data elements. However, there are several pieces of information that will be common among state systems. The types of information that will usually be obtained include--

- The client's name, address, and social security number
- The name, address, and social security number of the officers of participating retail food stores
- The client's income information (for program certification)
- The client's benefits system account number
- Data collected at the point of sale (time, location, amount, terminal number, retailer number)

Clearly, there are a variety of data elements that may be collected and shared at any stage of the process. Of course, not all such information will implicate privacy. For instance, the majority of retailer information collected is not personal and will not receive any protection under privacy laws.<sup>63</sup> Also, the degree to which information is shared will depend greatly on how that system is operated. A retail food store may collect information on what a client has purchased, but may, in fact, only use that information internally, if at all. Furthermore, just because the state collects information for certification purposes does not mean that that information will be available to any other party to the EBT process. In fact, as will be shown below, that is likely not to be the case.

---

<sup>62</sup> See *infra* Part II.

<sup>63</sup> That is not to say that commercial information is not protected as well; however, that protection is not the result of a privacy interest but of an interest in protecting confidentiality. Interestingly enough, the EBT regulations do provide protection for retailer information--above and beyond the protection of the *personal* information collected from retailers. See *infra* note 78 and the accompanying text for a discussion of the protections accorded retailer information.

### 3. *Users and uses of data*

In 1994, the USDA contracted to have a study performed regarding the privacy issues surrounding the use of EBT in the delivery of food stamps.<sup>64</sup> In this report, the authors identified the primary users and uses of data in the EBT program. Although some changes have been made to the program since then, this information is largely still accurate and serves as a secondary source for the following material. However, our preliminary research indicates that the details of the process may vary considerably among the states. Some states may design the system so that it isolates parties (e.g., the retail food store, the system operator) from certain identifying data elements. Others may allow parties to the EBT process to have more complete access to the information in the EBT databases, while using regulatory or contractual means to limit any disclosure to non-EBT parties. Therefore, the following description is at best a rough approximation of the process.

#### *a. Clients*

The first party to consider in the typical EBT transaction is the *client*. The client is the household that is eligible to participate in the Food Stamp Program.<sup>65</sup> The client submits an application to the state, which determines the client's eligibility. If the state finds that the client is eligible, then it issues an EBT card (usually a magnetic-stripe card<sup>66</sup>) and a personal identification number (PIN) to the client and establishes a food stamp account in the client's name.

#### *b. Retail food stores*

Once the client has an account and an EBT card, any authorized member of the household can use the EBT card to get food products from a *retail food store*.<sup>67</sup> Retail food stores must meet federal and state eligibility requirements. Participating retail food stores have point of sale terminals that can read EBT cards. These terminals, and the transaction process in general, are designed to reduce any potential stigma associated with being a food stamp recipient--to most observers, the transaction will look like any other credit or debit card transaction.

In an EBT transaction, the retail food store only acquires that data necessary to complete the transaction--for instance, the account number of the client. In general, the retail food store is not able to associate the account number or other collected data with the name of a specific client.

---

<sup>64</sup> See EBT DATA PRIVACY, *supra* note 5, at 1.

<sup>65</sup> *Client* is used in this report interchangeably for the recipient household and for an individual from that household.

<sup>66</sup> Ohio has used smart cards successfully in its pilot project. See *infra* Part II, section II.C.1.

<sup>67</sup> As defined in 7 C.F.R. § 271.2 (1998).

c. *Third party processors*

In states that use magnetic-stripe cards over an ATM network, retailers may rely on *third party processors* that have contracted with the state to handle the point of sale terminal operation or related services. Usually, these third party processors will be existing players in the commercial electronic funds transfer (EFT) network. As EBT transactions occur over the EFT network, the rules<sup>68</sup> that are agreed upon and adopted for managing these systems will be important--both for the protection of privacy and for the interoperability of systems among the states. However, for the most part, third party processors should, like retail food stores, have limited access to the identity of the client--they deal with account, retailer, and terminal numbers instead of personally identifiable information.

d. *The system operator*

There are a variety of ways that states can manage the statewide EBT system, but it appears at this stage that most states will contract with a *system operator* to handle this function. The most important role for the system operator is to authenticate each transaction, verifying that the client is authorized to use the card and that the client's account can cover the transaction.

The system operator may play a broader role in some states; in such cases, the amount of information accessible to the system operator will likely be greater. Depending on how much of the EBT system is controlled by the system operator, the system operator may have access to a great deal of personal information *and* the personal identifiers necessary to connect that information to a specific client.

e. *Concentrator banks*

Another party to the EBT process is the *concentrator bank*. The concentrator bank is "a member of the Federal Reserve System and has the capability to take information regarding retailer food stamp credits from the EBT system [operator] and transmit this information to the Automated Clearinghouse (ACH) network. The ACH transfers funds to and from member institutions and is the method used to credit retailers' accounts for food stamp EBT transactions".<sup>69</sup>

The concentrator bank is more involved with the flow of funds than with client-based information; therefore, the concentrator bank should have minimal, if any, access to personal information. As long as the account number and the information linking it to a client are segregated, then the opportunity for privacy protections to fail is minimized.

---

<sup>68</sup> The National Automated Clearing House Association (NACHA) has developed rules (the Quest rules) for governing these transactions, which states are in the process of adopting. See *Automated Clearinghouse (ACH) Rules* (last modified June 1, 1998)

<<http://www.nacha.org/resources/rules/default.htm/>>.

<sup>69</sup> EBT DATA PRIVACY, *supra* note 5, at 4.

Aside from the actual operation of the EBT system for transactions, the EBT regulations require a significant amount of data sharing to ensure that the system is operating efficiently and to prevent abuse of the system. This data sharing takes the form of reconciliation, system settlement, and exception reporting. Under the current scheme, most state EBT systems will not share personal information about the client to perform any of these functions.

*f. The USDA*

Although the USDA delegates a great deal of the operational management of the Food Stamp Program to the states, it does retain significant responsibilities in the areas of oversight, compliance, and enforcement. For the most part, these functions do not implicate privacy interests, but there are a few exceptions:

Retail Food Store Information

- The traditional role of the USDA has been, among other things, to ensure that retail food stores comply with program regulations and to prevent fraud by retailers. This investigative function is limited to tracking *retailer* information--client information is not usually collected by the agency. In fact, states generally handle *client* fraud with minimal USDA involvement.
- Most retail food store data is not personal information; however, some personal information is collected about the retail food store's owners and officers. This information is stored in the Store Tracking and Redemption Subsystem (STARS).<sup>70</sup>

Alien Status Verification

- Federal law requires that the Food Stamp Program participate in the Systematic Alien Verification for Entitlements (SAVE) Program. SAVE is an intergovernmental data-sharing system that allows agencies to identify the status of alien participants in benefits programs. This information allows agencies to determine whether an alien is eligible for any given benefits program.

---

70

The applications for authorization and reauthorization are in the STARS database and located in the files of FCS field offices. The applications contain the following personal information regarding owners and officers: Name, home address, social security number, and date of birth. Financial data (i.e., food sales, gross sales, food stamp redemption data) relative to each entity currently authorized or previously authorized is in the STARS database. While this information is not covered by the Privacy Act when associated with business information, it is subject to the Privacy Act when associated with the personal information of owners and officers of such entities.

61 Fed. Reg. 63, 815, 63, 816 (1996).

There are additional systems that operate in conjunction with STARS: the Retailer EBT Data Exchange System (REDE) and the Anti-fraud Locator of EBT Retailer Transactions (ALERT).

## Benefits Eligibility

- The State Income and Eligibility Verification System (IEVS) is "a system of information acquisition and exchange for purposes of income and eligibility verification".<sup>71</sup> Like other benefits programs, the Food Stamp Program contributes to and uses IEVS to verify that recipients are eligible for benefits.<sup>72</sup>

As mentioned above, the USDA does not regularly track recipient information. However, it should be noted that the EBT system makes the tracking of recipient transactions far more feasible than in the paper-based system.<sup>73</sup> Yet the mere capability to do this is not enough--federal law clearly limits the ability of *any* participant to disclose or use information outside of the Food Stamp Program, as shown below.

### 4. *Application of selected federal laws*

#### a. *Privacy Act of 1974*

The application of the Privacy Act to the program is fairly limited, and should remain so, even when EBT becomes the primary delivery mechanism for food stamps. The reason for this is simple: in general, the USDA will not be maintaining a real-time system of records on food stamp clients. On the other hand, data sharing involving the federal retailer information databases is controlled by the Privacy Act to the extent that these databases contain personal information (for instance, about retail food store officers). Also, the USDA will acquire a limited amount of client data when conducting fraud investigations. Since the traditional approach for the USDA has been to limit its investigations to retailers (leaving client-level investigations to the states), there should be only a small amount of client information in the hands of the USDA.

Although the states *will* be maintaining personal information about recipients while executing the federal program, a state agency is nonetheless *not* an "agency" by Privacy Act standards. Therefore, most of the "systems of records"--in fact, all databases maintained by the states--fall outside the scope of the Privacy Act.

However, there are a few ways that the Privacy Act may come into play, albeit indirectly. First, certain provisions of the Act may be incorporated into the regulations or contracts that govern EBT transactions. For example, the Federal Acquisition Regulations direct agencies to insert clauses that require contractors maintaining systems of records on behalf of an agency to adhere to the provisions of the Privacy

---

<sup>71</sup> 7 C.F.R. § 271.2 (1998).

<sup>72</sup> 7 C.F.R. § 273.2(f)(9) (describing the IEVS verification process).

<sup>73</sup> The EBT Data Privacy Report comes to a similar conclusion: "[USDA] regulation 274.12(h)(3)(v)(H) requires the State agency to assure the availability of a complete audit trail which 'shall, at a minimum, be able to provide a complete transaction history of each individual system activity that affects an account balance.' This necessarily involves identifying a POS transaction by account. The major privacy questions, then, involve what uses the government and retailers may make of household purchase information." See EBT DATA PRIVACY, *supra* note 5, at A-2.

Act.<sup>74</sup> While the Federal Acquisition Regulations do not apply directly to the states in the EBT roll out, they still establish a principle that states may follow.

Second, the Privacy Act is implicated when the federal government acquires information and maintains it in a system of records. This has already happened in the development of the USDA's database dealing with retailer data. Since the EBT program remains in a nascent stage, the full extent to which these systems of records will be used remains unclear.

Third, the possibility remains that the USDA will want to track transactions in real time at the client level. There are several entirely legitimate reasons why this might occur. The USDA may wish to move fraud enforcement from a retailer-based activity to a client-based one. Or it is possible that the USDA may track this information to ensure that food stamp purchases are meeting the nutritional goals of the program for each client. Although the USDA currently has no plans to do this sort of tracking, the possibility is worth noting because this kind of data sharing would likely cause the greatest concern among privacy advocates and the general public.

*b. USDA Food Stamp Regulations<sup>75</sup>*

The principal legal source for protecting privacy in the EBT program is the USDA Food Stamp Program regulations. These regulations set out, in a fair amount of detail, the requirements and the prohibitions that states must follow when administering the Food Stamp Program. The majority of the "protections" set out in these regulations deal with limiting access through system design and security measures, but several provisions stand out for their protection of privacy:

Disclosure Limits<sup>76</sup>

- The uses to which client (or applicant) information can be put are quite limited and are enumerated in the Food Stamp Program regulations. These disclosures are limited to--
  - Persons "directly connected with the administration or enforcement" of the Food Stamp or related benefits program
  - Persons "directly connected with the administration or enforcement" of the Income Eligibility Verification System, "to the extent the food stamp information is useful in establishing or verifying eligibility. . ."
  - Persons "directly connected with the verification of [the] immigration status of aliens<sup>77</sup> applying for food stamp benefits"

---

<sup>74</sup> 48 C.F.R. § 24.104 (1998).

<sup>75</sup> 7 C.F.R. § 271.1 (1998). Note that these regulations are the implementation of the Food Stamp Act of 1977, 7 U.S.C. § 2020, and the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Pub. L. No. 104-195, 100 Stat. 2105.

<sup>76</sup> 7 C.F.R. § 272.1(c) (1998).

<sup>77</sup> The Systematic Alien Verification for Entitlements (SAVE) program.

- Persons "directly connected with the administration of the Child Support Program. . ."
  - "Employees of the Comptroller General's Office" for auditing purposes.
  - "Local, State, or Federal law enforcement officials. . .for the purpose of investigating an alleged violation of the Food Stamp Act or regulation[s]"
  - Clients, upon request
- In addition, Section 272.1(c)(2) requires that authorized recipients of client information "must adequately protect the information against unauthorized disclosure to persons or for purposes not specified in this section".

### Protection of Retailer Information

- Section 278.1(r) strictly limits the disclosure of *retail food store* information. This information "may be disclosed to and used by Federal and State law enforcement and investigative agencies for the purpose of administering or enforcing the Food Stamp Act or any other Federal or State law, and the regulations issued under the Food Stamp Act or such other law".<sup>78</sup> However, the criteria governing such disclosures are quite restrictive, as are the types of disclosures permitted.

### State System Obligations

- The regulations governing the EBT program place a special burden on each state to guarantee that privacy protections for personal information are in place *before* each program begins operations.<sup>79</sup>
- The states also have an obligation to "ensure that third party processors and food retailers driving their own terminals comply with this section and all applicable Food Stamp Program regulations".<sup>80</sup> Presumably, this obligation compels each state to make sure that retail food stores and third-party processors are conforming with the privacy and security provisions of the Food Stamp Program regulations.

The degree to which these regulations actually protect privacy in the EBT program is still unclear. There remains a great deal of variety in how states are executing the program, and, for most states, the EBT program is still in a pilot phase. The second and third parts of this study will focus more directly on what the states are doing in practice.

---

<sup>78</sup> 7 C.F.R. § 278.1(r) (1998).

<sup>79</sup> 7 C.F.R. § 274.12(e) (1998):

(e) Functional Requirements. The State agency shall ensure that the EBT system is capable of performing the following functional requirements prior to implementation:

(1) . . .(ix) Ensuring the privacy of household data and providing benefit and data security. . . .

<sup>80</sup> 7 C.F.R. § 274.12(h)(5)(iii) (1998).

B. THE HHS CHILD SUPPORT ENFORCEMENT PROGRAM'S FEDERAL PARENT LOCATOR SERVICE/NATIONAL DIRECTORY OF NEW HIRES

1. *Program description*

The Child Support Enforcement Program is implemented by the Department of Health and Human Services (HHS) and is established under the Social Security Act as a Title IV-D Program, Grants to States for Aid and Services to Needy Families with Children and for the Child-Welfare Services, Child Support and Establishment of Paternity.<sup>81</sup>

The purpose of this program is to "enforc[e] the support obligations owed by noncustodial parents to their children and the spouse (or former spouse) with whom such children are living, locat[e] noncustodial parents, establish[ ] paternity, obtain[ ] child and spousal support, and assur[e] that assistance in obtaining support will be available to all children. . .for whom such assistance is requested."<sup>82</sup>

The principal program under the Child Support Enforcement umbrella for locating noncustodial parents is the Federal Parent Locator Service (FPLS). Under the FPLS are the Federal Case Registry of Child Support Orders and the National Directory of New Hires, which are programs that were created by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (Welfare Reform Act).<sup>83</sup> Each of these programs has been developed in order to expedite the process of locating a noncustodial parent for the payment of child support. One of the main characteristics of these programs is the requirement that data be shared between systems. It is interesting to note that the original collection of this data is done by the states, in a state system of records, and then transferred, as required by statute, to a federal system of records.

2. *Data elements*

The FPLS was created for the purpose of establishing parentage and establishing, setting the amount of, modifying, and enforcing child support obligations. The FPLS is used to obtain, or facilitate the discovery of, the location of any individual<sup>84</sup>--

- Who is under an obligation to pay child support
- Against whom an obligation is being sought
- To whom an obligation is owed

---

<sup>81</sup> 42 U.S.C. § 652 (1998).

<sup>82</sup> 42 U.S.C. § 651 (1998).

<sup>83</sup> Pub. L. No. 104-193, 100 Stat. 2105 (1996).

<sup>84</sup> 42 U.S.C. § 653a(2)(A) (1998).

This information is also used to enforce any federal or state law with respect to the unlawful taking or restraint of a child, or making or enforcing a child custody or child visitation determination.

The type of information that can be obtained includes--

- The individual's social security number (or numbers)
- The individual's most recent address
- The name, address, and employer identification number of the individual's employer
- Information on the individual's wages (or other income) and benefits from employment (including rights to or enrollment in group health care coverage)
- Information on the type, status, location, and amount of assets
- Information on debts owed by or to an individual

The law requires the disclosure of information in this database to authorized persons,<sup>85</sup> provided that such information is contained in any files or records maintained by HHS or can be obtained from any other department, agency, or instrumentality of the United States, or of any state, and is not otherwise prohibited from disclosure.<sup>86</sup>

*a. The National Directory of New Hires*

The information in this database is obtained directly from each State Directory of New Hires, except for federal agencies, which will report data directly to the National Directory.<sup>87</sup> The states will be required to collect the data and, in turn, to transmit the data to the National Directory. The National Directory will check the data from all the states for matches between noncustodial parents and new hires and then transmit the matched information to the appropriate state. The National Directory is also required to provide all information collected to the Social Security Administration.<sup>88</sup>

The law requires all employers (as defined by section 3401(d) of the Internal Revenue Code of 1986), to furnish the following information to the Directory of New Hires in the state where a newly-hired employee works:<sup>89</sup>

- Employee name
- Employee address
- Employee social security number
- Employer name
- Employer address
- Employer identification number

---

<sup>85</sup> 42 U.S.C. § 653c.

<sup>86</sup> 42 U.S.C. § 653b(2).

<sup>87</sup> 42 U.S.C. § 653i.

<sup>88</sup> 42 U.S.C. § 653j(3)(B).

<sup>89</sup> 42 U.S.C. § 653a (b)(1)(A).

Employers must provide this information to their state's directory under the time frames indicated in the regulations--from two to twelve days.

The State Directory of New Hires, as required under the Welfare Reform Act, has two implementation dates. For those states that had no directory in place, an automated directory was required to be in place and in compliance with federal requirements by October 1, 1997. For each state that already had a new hire reporting law, the state could continue to operate under its own law, but it had to meet the requirement of transmitting the information to the National Directory by October 1, 1997, and has to meet the remainder of the requirements under federal law by October 1, 1998.

Employers are further required to report to the state the quarterly wages of all employees. Wage information from agencies administering state unemployment compensation are to be made available to the State Directory as part of the income eligibility and verification system for federal benefits.<sup>90</sup> The state must then provide wage and unemployment compensation information to the National Directory of New Hires on a quarterly basis. All information provided by the states is subject to the Privacy Act once that information becomes part of a federal system of records, but it is not subject to the Privacy Act as part of a state system of records.

*b. Federal Case Registry of Child Support*

This program is not required to be operational until October 1, 1998. The Registry contains abstracts of support orders and other information with respect to each child support case and order in each state case registry. Information collected will include--

- Name
- Social security number (or other identification number)
- State case identification number
- Individuals who owe support or to whom support is owed
- State or states that have the case or order

*3. Users and uses of data*

Under the HHS Privacy Act regulations,<sup>91</sup> a routine use of data is defined as "the disclosure of a record outside the Department, without the consent of the subject individual, for a purpose which is compatible with the purpose for which the record was collected. . .".<sup>92</sup> Most data sharing uses between agencies are identified as being a routine use, although under the regulations of the FPLS for the National Directory of

---

<sup>90</sup> 42 U.S.C. § 1302b-7(b) (1998).

<sup>91</sup> 45 C.F.R. § 5b.1 (1998).

<sup>92</sup> 45 C.F.R. § 5b.1(j).

New Hires, the data to be shared and those agencies eligible for data sharing are expressly identified.<sup>93</sup>

a. *Routine uses*

1) *Federal Parent Locator Service (FPLS) and the National Directory of New Hires (NDNH)*

The current published routine uses for systems of records under the FPLS include--

- Requesting the most recent home and employment addresses and social security numbers (SSNs) of the noncustodial parents from any state or federal government department, agency, or instrumentality that might have such information in its records
- Providing the most recent home and employment addresses and SSNs to state Child Support Enforcement (CSE) agencies (as well as to the FBI and the Center for Missing and Exploited Children), for the purpose of locating noncustodial parents in connection with establishing or enforcing child support obligations
- Providing the most recent home and employment addresses and SSNs to state CSE agencies under agreements covered by section 463 of the Social Security Act for the purpose of locating noncustodial parents or children in connection with activities by state courts and federal attorneys and agents charged with making or enforcing child custody determinations or conducting investigations, enforcement proceedings, or prosecutions concerning the unlawful taking or restraint of children
- Providing the most recent home and employment addresses and SSNs to agents and attorneys of the United States involved in activities in states that do not have agreements under section 463 of the Act for purposes of locating noncustodial parents or children in connection with federal investigations, enforcement proceedings, or prosecutions involving the unlawful taking or restraining of children
- Providing to the State Department the names and SSNs of noncustodial parents in international child support cases and in cases involving the Hague Convention on the Civil Aspects of International Child Abduction<sup>94</sup>

The Welfare Reform Act amended the federal law and authorized new uses and disclosures for the expanded FPLS, which includes the National Directory of New Hires. The new routine uses for this system include the following:

- State agencies may access data in the National Directory of New Hires (NDNH) for the purpose of administering the CSE program and the Temporary Assistance for Needy Families (TANF) program.
- The Commissioner of Social Security may access information in the NDNH for the purpose of verifying reported SSNs and for other purposes.

---

<sup>93</sup> 42 U.S.C. § 653j.

<sup>94</sup> 62 Fed. Reg. 51, 665, 51, 668 (1997).

- The Secretary of the Treasury may access information in the NDNH for the purposes of administering advance payment of the earned income tax credit and verifying a claim with respect to employment in a tax return.
- The Secretary of HHS may provide researchers with access to the new hire data for research efforts that would contribute to the TANF and CSE programs. Information disclosed may not contain personal identifiers.
- Records may be disclosed to any agent of any agency that is under contract with the state CSE agency to assist in locating individuals for the purposes of establishing, modifying, and enforcing child support.
- Records in the NDNH may be disclosed to state CSE agencies in order to locate individuals for the purpose of establishing paternity and for the establishment, modification, or enforcement of a support order.
- Records may be disclosed to state CSE agencies that need to locate individuals for the purpose of enforcing child custody and visitation orders.
- New hire information may also be disclosed to the state agency administering the Medicaid, Unemployment Compensation, Food Stamp, SSI, and territorial cash assistance programs for income eligibility verification, and to state agencies administering unemployment and workers' compensation programs to assist determinations of the permissibility of claims.
- The CSE program office will disclose information to the Treasury Department for the offset of certain federal payments in order to collect past due child support obligations. Federal payments included in this type of disclosure are--
  - Federal salary, wage, and retirement payments
  - Vendor payments
  - Expense reimbursement payments
  - Travel payments
- Information from FPLS may be disclosed to the Secretary of State to revoke, restrict, or deny a passport to any person certified by state CSE agencies as having a child support arrearage greater than \$5,000.00.<sup>95</sup>

The notice in the Federal Register also provides language on the use of new hire data by federal and state personnel and contractors, requiring them to adhere to the provisions of the Privacy Act and the HHS Privacy Act regulations.<sup>96</sup>

## 2) *State Directory of New Hires*

The information located in the state directories is to be provided to the National New Hire Directory, but other uses established under the statute include--

---

<sup>95</sup> *Id.*

<sup>96</sup> *Id.* at 51, 665.

- Location of child support obligors. States may use this information to locate individuals for the purposes of establishing paternity and establishing, modifying, and enforcing child support obligations.
- Verification by a state agency of eligibility of certain programs. A state agency shall have access to information reported by employers for the verification of eligibility.
- Administration of employment security and workers' compensation by the administering state agency. State agencies have access to the State Directory to administer the employment security and workers' compensation programs.<sup>97</sup>

*b. Data sharing*

Under the Federal Parent Locator Service, provisions for the National New Hire Directory require the sharing of data with other agencies. These provisions include providing the information to--

- The Secretary of the Treasury for administration of tax laws
- The Social Security Administration for verification of the name, social security number, and date of birth of each individual and the employer identification number of the individual's employer
- Use for matching against the Federal Case Registry of Child Support Orders
- Use for information comparisons and disclosures of information in all registries for Title IV program purposes<sup>98</sup>

*4. Application of federal laws*

*a. Privacy Act of 1974*

The use of data in a federal system of records is restricted by the requirements of the Privacy Act of 1974. All information obtained from the states under the requirements of the Child Support Enforcement Services and submitted to any of the federal programs becomes subject to the Privacy Act once the information becomes a part of a federal system of records established for use by HHS.

*1) System of records*

HHS is required to publish a notice of a change to a system of records or the creation of a new system of records in the Federal Register. Such a notice was published for a change in the FPLS system of records that was needed to comply with the Welfare Reform Act, in August 1997. The final notice was published in the Federal Register in October 1997. This notice outlines the components of the system of records, including--

---

<sup>97</sup> 42 U.S.C. § 653a(h).

<sup>98</sup> 42 U.S.C. § 653 (i)(j).

- Employment data on newly-hired employees submitted by the State Directories of New Hires
- Quarterly Wage information on individual employees submitted by the states, and quarterly wage information of federal employees submitted by federal agencies
- Unemployment compensation claims data submitted by the states

As required under the Privacy Act, this notice also identifies the categories of individuals covered by this system of records and the categories of records or data elements that were collected. Not only has the FPLS been expanded pursuant to the provisions of the Welfare Reform Act that amended the Social Security Act, but it has also been expanded by the Debt Collection Improvement Act of 1996<sup>99</sup> and by Executive Order 13019.<sup>100</sup> These provisions have given HHS the authority to expand the FPLS to improve the states' ability to locate noncustodial parents and to collect child support. The National Directory of New Hires was established to provide interstate matching of child support obligors and employment, earnings, and benefit data and to promote a more efficient flow of data between states.

*b. The HHS Privacy Act Regulations<sup>101</sup>*

To comply with the Privacy Act, HHS has included privacy provisions in its regulations. These regulations provide guidance for systems of records, routine uses, policies and procedures for the maintenance of records, disclosures of records, and most importantly, a policy statement on privacy. The HHS privacy policy is to protect the privacy of an individual's information while allowing for the exchange of data that is necessary to fulfill the administrative and programmatic responsibilities of the Department.<sup>102</sup>

*c. State obligations*

Because the states administer the federal programs, they can only use and disclose program information as provided in the HHS regulations. Each state is required to submit a state plan, which is a comprehensive statement describing the nature and scope of the program and which provides assurance that the state plan will

---

<sup>99</sup> Pub. L. No. 104-134, 110 Stat. 1321-373 (1996).

<sup>100</sup> Supporting Families: Collecting Delinquent Child Support Obligations, Exec. Order No. 13, 019, 61 Fed. Reg. 51, 761 (1996).

<sup>101</sup> 45 C.F.R. § 5b.1 - 5b.13.

<sup>102</sup> 45 C.F.R. § 5b.3.

be administered in conformity with the specific requirements of the HHS regulations.<sup>103</sup> The purpose of the state plan is to assure HHS that the state program meets the federal criteria for administering the program. The plan is the basis for federal financial support of the state program. How the states comply with these regulations will be further investigated in the second and third parts of this study.

---

<sup>103</sup> See Title IV-D and the regulations in subchapter A of 45 C.F.R. that include the privacy provisions. 45 C.F.R. § 301.10 (1998).

## **PART II: THE LEGAL FRAMEWORK OF PRIVACY – THE STATE AND LOCAL SYSTEMS**

### **I. INTRODUCTION TO STATE ISSUES**

The role of the states in operating federal programs varies from program to program. Therefore, the information acquired about the EBT and Child Support Enforcement databases cannot be considered as necessarily representative of data-sharing programs in general. In fact, both programs deal with particularly sensitive information and may have greater protections at the state and federal level than do other data-sharing programs.

The federal Privacy Act and the agency regulations set the minimum level of privacy protection. As mentioned in Part I of this study, each program expressly imposes limits on the kinds of disclosures that can be made in the operation of the program. State laws can only increase this protection; however, the variance of the protections provided by the states may be considerable. This variance could, in the long run, be a significant barrier to the overall interoperability of state EBT systems. This is less of a problem with the National Directory of New Hires.

When looking at state laws, we will not discuss those laws that simply reinforce the federal program requirements except to the extent that state law significantly exceeds federal requirements. However, it should be noted that a state law providing for the protection of personal information can--and often does--create a separate state cause of action for an individual whose informational privacy rights were violated.

To the greatest extent possible, this part of the study relies on information acquired directly from officials from the five selected states. However, we used legal and Internet-based research to supplement and verify the information, whenever possible. For the occasions when we were unable to locate information or lacked a resource, we note the absence below.

### **II. STATE LAWS AND PRACTICES RELATED TO CASE STUDY PROGRAMS**

#### **A. KANSAS**

## KANSAS EBT FACTS

<b>Statistics</b>	
No. of Food Stamp Program Households	53, 916 <sup>104</sup>
No. of EBT Households	53, 916 <sup>105</sup>
No. of Authorized Retail Food Stores	1, 267 <sup>106</sup>
<b>Alliance</b>	None <sup>107</sup>
<b>EBT Deployment Status</b>	Statewide <sup>108</sup>
<b>System Operator</b>	Deluxe Data <sup>109</sup>
<b>Administering Agency</b>	Dept. of Social and Rehabilitation Services

### 1. Overview of the state's EBT program

Kansas has opted for a multiple benefit EBT system operated over the state's ATM network. The client, once he qualifies for the Food Stamp Program, receives a magnetic-stripe card and a personal identification number (PIN).

When Kansas began its EBT program, the program planners made a conscious decision to minimize the amount of information accessible by participants<sup>110</sup> to the EBT process. This decision reflected an emphasis on recipient privacy that had existed in the paper coupon system.

In Kansas, the system operator<sup>111</sup> receives from the state several data elements for each client: a card number, name, and date of birth. The system operator does not receive the address or social security number of the client. Through the operation of the program, the only additional data that the system operator receives is the location and name of the retail food store where the client made his purchase.

For the retailer, even less information is available. The retailer only gets the EBT card number. Although this number is tied to the state's case number (the personal identifier for the state database), the retailer has no access to the state database and, therefore, has no way of matching the card number up with any personal information. The clerk at the retailer's point of sale can see the name of the client, because the name

<sup>104</sup> U.S. DEP'T OF AGRIC., ESTIMATED EBT CONTRACTOR ROLL-OUT NUMBERS BY STATE 2 (May 14, 1998) <<http://www.usda.gov/fcs/stamps/rollout.pdf>>.

<sup>105</sup> *Id.*

<sup>106</sup> U.S. DEP'T OF AGRIC., FOOD STAMP PROGRAM ELECTRONIC BENEFITS (EBT) PROJECT STATUS HIGHLIGHTS 11 (March 1998) <<http://www.usda.gov/fcs/stamps/ebtstat.doc>>.

<sup>107</sup> Kansas was in the Southwest Consortium but withdrew. *Id.*

<sup>108</sup> *Id.* at 1. Kansas reached statewide implementation in March 1997. *Id.* at 11.

<sup>109</sup> *Id.*

<sup>110</sup> "Participants", as used in Part II of this study in reference to the EBT program, refers more to retail food stores, system operators, state agencies, third-party processors, and other operations-oriented parties than to clients (food stamp recipients).

<sup>111</sup> See *supra* Part I, section IV.A.3.d., to review the system operator's role in the EBT program.

is on the EBT card; however, the name is not used in the transaction itself, nor does the retailer record it in the course of the transaction.

As referred to in the preceding paragraph, Kansas maintains a benefits database with personal information, but this information can only be accessed by authorized state officials for program or program-related purposes. In fact, even though the state agency knows the identity of the client in any given case, it will not give that client's personal information to the retailer or to the system operator for any purpose.

Kansas reported no known major privacy problems in the operation of its system.

## 2. *Overview of the state's New Hire Directory*

The legislature in Kansas designated the Department of Human Resources as the agency to collect the new hire information required by the federal legislation.<sup>112</sup> The Child Support Enforcement Agency is a division of this Department. Kansas had a new hire program in place before the federal requirements were mandated, although the information was collected by the Workers' Compensation Department. The new statute outlines the requirements found in the federal law, expands the data elements that were previously being collected, and requires employers to report new hires and quarterly wage information. This statute also stipulates that any agency receiving information from the state directory shall treat the information as confidential.<sup>113</sup>

New hire information is reported directly from the employers to the Department of Human Resources. The Department does all data entry, formatting and compiling of the information. By Kansas statute, the Child Support Enforcement division does not have direct access to the data in the new hire data base, but "[t]he state directory of new hires shall make information available to the secretary of social and rehabilitation services for use in administering an eligibility verification system and. . .the title IV-D program."<sup>114</sup> Child Support Enforcement information is transmitted by file transfer to the Department of Human Resources for matching. The data matching is done on a weekly basis and a report of all matches is returned to Child Support.

As an additional safeguard, Child Support Enforcement employees are required to sign a confidentiality statement/security agreement when hired to confirm their responsibility to protect the confidentiality of records.

Kansas uses Connect: Direct to transmit the information from the state database to the federal database. Connect: Direct uses Internet protocol and encryption methodology to ensure the security of the data being transmitted. It is intended to be a secure line for transmission directly to the federal database.

Kansas reported no known major privacy problems in the operation of its system.

---

<sup>112</sup> KAN. STAT. ANN. § 75-5742(a) (1997).

<sup>113</sup> KAN. STAT. ANN. § 75-5742(c).

<sup>114</sup> KAN. STAT. ANN. § 75-5742 (c)(2).

3. *Selected state legal and regulatory issues*

a. *Informational privacy in the state constitution*

The Kansas Constitution does not specifically provide for the protection of informational privacy.

b. *Omnibus privacy act*

Kansas does not have an omnibus privacy act.

c. *Public records law*

The Kansas Open Records Act states that it is "the public policy of the state that public records shall be open for inspection by any person unless otherwise provided by this act, and this act shall be liberally construed and applied to promote such a policy".<sup>115</sup> Therefore, like the federal Freedom of Information Act, the important question in Kansas is whether information constitutes a public record or is exempted by the Act. As it turns out, the records that are created through the EBT program are almost certainly exempted:

"Except to the extent disclosure is otherwise required by law, a public agency shall not be required to disclose. . . [r]ecords the disclosure of which is specifically prohibited or restricted by federal law. . . or the disclosure of which is prohibited or restricted pursuant to specific authorization of federal law. . . ." <sup>116</sup>

Although this provision adds little to the privacy equation--the federal prohibitions would hold regardless of what Kansas law states--it does help to make clear to state officials that the limitations of the Food Stamp Program are incorporated by reference into state law.

d. *State EBT and CSE program and welfare-related regulations*

The Kansas welfare statutes have a general provision for protecting the confidentiality of recipient information. In particular, "[i]nformation concerning applicants for and recipients of assistance from the secretary shall be confidential and privileged".<sup>117</sup> The exceptions where disclosure is permitted are few and fairly straightforward (e.g., for the direct administration of the program<sup>118</sup> or for law

---

<sup>115</sup> KAN. STAT. ANN. § 45-216(a).

<sup>116</sup> KAN. STAT. ANN. § 45-221(a)(1).

<sup>117</sup> KAN. STAT. ANN. § 39-709b(a).

<sup>118</sup> KAN. STAT. ANN. § 39-709b(a)(3)(B).

enforcement investigations connected with the administration of the program<sup>119</sup>), with one exception--a public list of welfare recipients.

In Kansas, the welfare department is required to maintain a public list of the names and addresses of persons receiving public assistance.<sup>120</sup> However, it is against the law for any "person, association, firm, corporation or other agency" to disclose the names on the list for "commercial or political purposes" or to disclose any confidential information about recipients without legal authority.<sup>121</sup> This law could help to fill any gaps in the federal program regulations vis-à-vis private parties since this section applies to the private sector as well as to government.<sup>122</sup>

Another interesting provision in Kansas law is section 39-759 under the Social Welfare article, which describes unlawful acts relating to information concerning absent parents. "[A]ny person who willfully requests, obtains or seeks to obtain confidential information under false pretenses or who willfully communicates or seeks to communicate such information to any person except in accordance with any law permitting such disclosure shall be guilty of a severity level 10, nonperson felony."<sup>123</sup> The statute further provides for the immediate dismissal of the individual if the offender is an officer or employee of the state, and if the offender's supervisor does not dismiss the offender, the supervisor will also be dismissed. The statute also pertains to contractors in the Title IV-D (Child Support) program and violation of this section is grounds for the termination of a contract.

e. *Contract provisions*

The standard retailer agreement used in Kansas has a confidentiality clause that limits the ability of a retailer to disclose information acquired through the EBT program. As for the state's agreement with the system operator, it is reported that the agreement addresses confidentiality issues but does not include a comprehensive confidentiality clause.

The collection of data for the new hire directory is done through a state agency; therefore, there are no third-party contractors involved.

---

<sup>119</sup> KAN. STAT. ANN. § 39-709b(a)(3)(C).

<sup>120</sup> KAN. STAT. ANN. § 39-709b(c).

<sup>121</sup> KAN. STAT. ANN. § 39-709b(d).

<sup>122</sup> On the other hand, the law may violate the First Amendment. See *infra* Part III, section II.A.10.

<sup>123</sup> KAN. STAT. ANN. § 39-759(a).

B. MARYLAND

**MARYLAND EBT FACTS**

<b>Statistics</b>	
Number of Food Stamp Program Households	144, 200 <sup>124</sup>
Number of EBT Households	144, 200 <sup>125</sup>
Number of Authorized Retail Food Stores	3, 057 <sup>126</sup>
<b>Alliance</b>	Mid-Atlantic Regional Coalition <sup>127</sup>
<b>EBT Deployment Status</b>	Statewide <sup>128</sup>
<b>System Operator</b>	Deluxe Data <sup>129</sup>
<b>Administering Agency</b>	Dept. of Human Resources

1. *Overview of the state's EBT program*

Maryland was the first state to launch a statewide multiple benefit EBT program.<sup>130</sup> Thus, in many ways, the Maryland experience has served as a model for other states' EBT programs. The Maryland program, like the Kansas program, operates over the commercial ATM network and uses a magnetic-stripe card in conjunction with a PIN.

Maryland has taken strong measures to minimize the sharing of personal information. Participants in the EBT program only receive the bare minimum of information needed to complete an EBT transaction. In fact, state officials themselves rarely access eligibility data;<sup>131</sup> generally, they limit their access to operations data.<sup>132</sup>

When a client is declared eligible for public assistance, the state issues an authorization number for each benefit type. A case number and an EBT card number are also created and are tied to the authorization number. The system operator only gets the case number and the funds available for that case number. The system operator does not know who the client is, and it is not allowed to attempt to contact the client.

<sup>124</sup> ESTIMATED EBT CONTRACTOR ROLL-OUT NUMBERS BY STATE, *supra* note 104, at 2.

<sup>125</sup> *Id.*

<sup>126</sup> FOOD STAMP PROGRAM EBT PROJECT STATUS HIGHLIGHTS, *supra* note 106, at 13.

<sup>127</sup> *Id.*

<sup>128</sup> *Id.* at 1. Maryland reached statewide implementation in April 1993. *Id.* at 13.

<sup>129</sup> *Id.*

<sup>130</sup> U.S. DEP'T OF AGRIC., FINAL RESULTS: THE EVALUATION OF THE MARYLAND EBT DEMONSTRATION 1 (May 25, 1994).

<sup>131</sup> Eligibility data is the data collected when the client first applies for public assistance. The state acquires the bulk of the personal information collected (and associated personal identifiers) through this process.

<sup>132</sup> Operations data is data used for processing transactions. This data contains far less personal information than eligibility data.

The retailer gets very little information in an EBT transaction. There is no information exchanged that can reasonably be tied to any client. In fact, the retailer does not even learn the balance of the account--the transaction either is approved or not is approved by the system.

Maryland reported no known major privacy problems in the operation of its system.

## 2. *Overview of the state's New Hire Directory*

Maryland operated a voluntary new hire reporting system that lasted through the 1980s until 1996. In 1996, Maryland's new hire reporting became mandatory, and the state was in the process of revising its registry when the federal government intervened with its new requirements for a national new hire database. As a result, Maryland law was modified to fulfill the federal requirements for a state directory of new hires and was adopted in 1997.<sup>133</sup> This new statute does not specifically use the phrase "new hire database" or any other terminology found in other jurisdictions. What this statute does do is outline the requirements for reporting by employers. The statute requires the information to be submitted to the Secretary of Labor, Licensing, and Regulations<sup>134</sup> but requires the Department of Human Resources to reimburse Labor, Licensing, and Regulations for the cost of implementing the system.<sup>135</sup>

Because the system was created for the use of the Child Support Enforcement Agency, the Department of Human Resources has taken on the responsibility for the system. The Department of Labor, Licensing, and Regulations and the Department of Human Resources are currently in the process of creating an interagency agreement to transfer some responsibilities from Labor to Human Resources.

Maryland uses a contractor to collect new hire information from employers. This information is maintained in the database developed by the contractor. The contractor is required to transmit the information to the following agencies:

1. The Maryland Department of Human Resources/Child Support Enforcement
2. The Maryland Department of Labor, Licensing, and Regulations for Unemployment Insurance
3. The U.S. Department of Health and Human Services/National Directory of New Hires

The contractor does not transmit information to any other agency databases. The departments match their data to the data sent by the contractor. The Child Support Division receives its data in batch format nightly and matches are performed daily from the new information. There is no matching agreement needed in the transfer of data to agencies from the new hire database, because this activity is covered by the contract

---

<sup>133</sup> MD. CODE ANN., Labor and Employment § 8-626.1.

<sup>134</sup> MD. CODE ANN., Labor and Employment § 8-626-1(b).

<sup>135</sup> MD. CODE ANN., Labor and Employment § 8-626-1(f).

between the contractor and the state. New hire information is only transmitted to those agencies permitted by law to receive the information.

Like Kansas, Maryland uses Connect: Direct to transmit new hire information to the federal database. Maryland reported no known major privacy problems in the operation of its system.

3. *Selected state legal and regulatory issues*

a. *Informational privacy in the state constitution*

The Maryland Constitution does not specifically provide for the protection of informational privacy.

b. *Omnibus privacy act*

Maryland does not have an omnibus privacy act.

c. *Public records law*

Maryland's public records law states that disclosure of public records is favored, "unless an unwarranted invasion of the privacy of a person in interest would result. . .".<sup>136</sup> Maryland law also limits the extent to which personal information can be held by government: "The State. . .may keep only the information about a person. . .that is authorized or required to be accomplished under [law] and. . .is relevant to the accomplishment of the purpose".<sup>137</sup> Furthermore, Maryland requires that public records shall *not* be disclosed if "by law, the public record is privileged or confidential or. . .the inspection would be contrary to. . .a federal statute or a regulation".<sup>138</sup> Indeed, in addition to this general provision, there is also a specific provision for preventing the disclosure of welfare records: "A custodian shall deny inspection of public records that relate to welfare for an individual".<sup>139</sup>

Although Maryland does not have a comprehensive "privacy act", it does have several statutes dealing with personal records held by government in its public records law.<sup>140</sup> This law establishes some procedures for handling personal records (e.g., reporting requirements and use of personal records for research) and creates civil and criminal liability for the willful and unlawful disclosure or use of personal information.<sup>141</sup> This liability extends to government officials and to private individuals.

---

<sup>136</sup> MD. CODE ANN., State Government § 10-612(b) (1997).

<sup>137</sup> MD. CODE ANN., State Government § 10-602(1)-(2).

<sup>138</sup> MD. CODE ANN., State Government § 10-615(1)-(2)(ii).

<sup>139</sup> MD. CODE ANN., State Government § 10-616(c).

<sup>140</sup> MD. CODE ANN., State Government § 10-624.

<sup>141</sup> MD. CODE ANN., State Government § 10-626 (civil liability) and § 10-627 (criminal liability).

d. *State EBT and CSE program and welfare-related regulations*

Maryland law makes it "unlawful for any person or persons to divulge or make known in any manner any information concerning any applicant for or recipient of social services, child welfare services, [or] food stamps".<sup>142</sup> There are only a few exceptions to this law, the most relevant being such disclosures that are "necessary to discharge responsibilities to administer public assistance. . .or social services programs. . .". This criminal liability applies equally to government officials and private individuals.

The Maryland food stamp law also requires that state and county agencies conform to any applicable federal laws or regulations, including, of course, the federal regulations concerning disclosures of client information.<sup>143</sup>

e. *Contract provisions*

In the system operator agreement and in the standard retailer agreement, Maryland has included nondisclosure requirements for the protection of personal (and other) information acquired in the execution of the program.

The standard services contract used by the Child Support Enforcement Administration and its contractors does not contain explicit language for the protection of confidential information used in connection with the contract. The agreement has a provision for "compliance with laws" that requires the contractor to comply with all federal, state, and local laws, regulations, and ordinances applicable to its activities and obligations under the contract.

C. OHIO

---

<sup>142</sup> MD. CODE ANN., art. 88A § 6.

<sup>143</sup> MD. CODE ANN., art. 88A § 88.

## OHIO EBT FACTS

<b>Statistics</b>	
Number of Food Stamp Program Households	332, 913 <sup>144</sup>
Number of EBT Households	50, 000 <sup>145</sup>
Number of Authorized Retail Food Stores	6, 393 <sup>146</sup>
<b>Alliance</b>	Mid-Atlantic Regional Coalition/Midwestern Alliance of EBT States <sup>147</sup>
<b>EBT Deployment Status</b>	Expanding statewide <sup>148</sup>
<b>System Operator</b>	Citibank <sup>149</sup>
<b>Administering Agency</b>	Dept. of Human Services

### 1. Overview of the state's EBT program

Ohio's EBT program is of particular interest because Ohio is one of two states with an off-line food stamp EBT program.<sup>150</sup> This "off-line" system uses a card with an embedded microchip--a smart card--rather than a card with a magnetic stripe, as used in on-line systems.<sup>151</sup> Although a smart card looks quite like a magnetic-stripe card, there is very little functional similarity between the two systems. In essence, a magnetic-stripe card is used to establish a connection to a centralized database. That database contains virtually all of the information relevant to the transaction--from the account number to the amount of money in the account. In addition, in a magnetic-stripe card transaction, the central database changes the account information to reflect the transaction--the card itself remains unchanged.

A smart card is fundamentally different. It relies on a microchip built into the card. Instead of being used to communicate with a database across a network, a smart card simply communicates authorization and account information to the terminal at the store. The changes in the user's account actually occur on the card itself. The store will reconcile the transaction (along with any other smart card transactions) with the bank or other crediting institution on a periodic basis. Another advantage of the smart card is that it limits the amount of information that needs to be exchanged in a transaction. All that the retailer needs to know (and all that the retailer gets) is the fact that the account is authorized and the account balance was sufficient to cover the items purchased.

---

<sup>144</sup> ESTIMATED EBT CONTRACTOR ROLL-OUT NUMBERS BY STATE, *supra* note 104, at 3.

<sup>145</sup> *Id.*

<sup>146</sup> FOOD STAMP PROGRAM EBT PROJECT STATUS HIGHLIGHTS, *supra* note 106, at 20.

<sup>147</sup> *Id.*

<sup>148</sup> *Id.* at 3. Ohio expects to reach statewide implementation by 1999. *Id.* at 20.

<sup>149</sup> *Id.*

<sup>150</sup> The other state with an off-line program is Wyoming. *Id.* at 3. See generally OHIO DEP'T OF HUM. SERVICES, LONG RANGE INFORMATION SYSTEMS PLAN (Oct. 1996) <[http://www.state.oh.us/opp/policy\\_pdfs/HUM-IT.PDF](http://www.state.oh.us/opp/policy_pdfs/HUM-IT.PDF)>.

<sup>151</sup> It should be noted that the Ohio smart card is issued with a personal identification number (PIN) which is actually embedded on the card (in encrypted form). This provides additional security and limits some kinds of fraud.

Ohio has considered privacy issues throughout the design and execution of its EBT program. In the paper coupon system, a party with access to one piece of client information would generally have access to *all* of it. However, the designers of the Ohio system realized that the data elements could be segregated in an electronic system. Taking advantage of this new capability, Ohio has designed its EBT program to minimize the amount of information disclosed--even information disclosed to parties *within* the EBT system. There are a number of ways that Ohio has designed its system to protect client information:

- The system operator has access to only a few data elements--case number, benefit available date, benefit amount. Recipient identification is encrypted. Since only state agencies have access to the database that matches the case number with the identity of the client, the system operator has no access to the client's name or other personal identifier.
- Transmissions of data across the EBT network are encrypted.
- The retailer has access to very little information about the client--the account balance is the only information on the receipt.

As a result of Ohio's effort to design the system to protect personal information, its EBT program actually exceeds the minimums set by the federal program regulations. By limiting the ability of any party to the EBT process (other than the state) to link transaction information with an individual, the possibility of unauthorized disclosures of such information is curtailed.

Ohio reported no known major privacy problems in the operation of its system.

## 2. *Overview of the state's New Hire Directory*

Under the Ohio Revised Code, the Department of Human Services is the agency assigned to administer the new hire database in Ohio. The Code states that "[e]very employer shall report the hiring, rehiring, or return to work of an employee. . . ."<sup>152</sup> This statute encompasses all the required data elements of the federal law. The statute also specifically states that the reports received under this section shall not be considered public records for purposes of section 149.43 of the revised code. It further states that disclosure of the information in the reports is available only to agents of the department or child support enforcement agencies under contract with the department. Finally, the law requires that a copy of the report from the employer may be submitted to the Bureau of Worker's Compensation or Bureau of Employment Services.<sup>153</sup> This law makes it clear that any information retained in the new hire database is not considered a public record.

Ohio uses a third-party contractor for the collection of the new hire database information from employers. This contractor does the data entry, converts the data into

---

<sup>152</sup> OHIO REV. CODE ANN. § 5101.312(B)(1) (Anderson 1998).

<sup>153</sup> OHIO REV. CODE ANN. § 5101.312(F).

a flat file, and transmits it nightly to the new hire database at the Department of Human Services. The contractor must comply with the privacy/confidentiality provisions that are contained in the federal and state laws.

The new hire data is housed with Child Support Enforcement data and Ohio Parent Locator Service data. All of this data is contained in a statewide database that is accessible by all county child support agencies and human services agencies. There are two methods available for extracting data from the system: (1) submitting tapes with the requests for automatic processing and (2) requesting a manual match through the parent locator service. For requests through the parent locator service, matches are done nightly. Requests submitted on tape are done monthly.

Ohio uses Connect: Direct to submit the information to the National Directory of New Hires. Ohio reported no known major privacy problems in the operation of its system.

### 3. *Selected state legal and regulatory issues*

#### a. *Informational privacy in the state constitution*

The Ohio Constitution does not specifically provide for the protection of informational privacy.

#### b. *Omnibus privacy act*

Ohio has long had an omnibus privacy act, with provisions similar to the federal Privacy Act.<sup>154</sup> For the most part, the Ohio Privacy Act simply reinforces the requirements of the federal programs' regulations. However, because the federal Privacy Act does *not* apply to the states, the existence of a state equivalent to the Act does create additional procedural protections for personal information collected and used by the state. Whether these provisions provide any real substantive advantage over and beyond the federal program requirements is uncertain.

The Ohio Privacy Act does impose, among other things, an affirmative obligation on state and local agencies to prevent unauthorized disclosures of personal information.<sup>155</sup> It also provides guidelines for oversight and for the security of any personal information system.<sup>156</sup> In addition, the Ohio Privacy Act imposes liability on state and local officials who harm individuals through the intentional illegal disclosure or misuse of personal information.<sup>157</sup> An agency that is involved in such harmful activities can be enjoined by a court of law.<sup>158</sup>

---

<sup>154</sup> OHIO REV. CODE ANN. § 1347.01.

<sup>155</sup> OHIO REV. CODE ANN. § 1347.05.

<sup>156</sup> OHIO REV. CODE ANN. § 1347.05.

<sup>157</sup> OHIO REV. CODE ANN. § 1347.10. There is also criminal liability for misuse of personal information by a government official in Ohio. OHIO REV. CODE ANN. § 1347.99.

<sup>158</sup> OHIO REV. CODE ANN. § 1347.10(B).

c. *Public records law*

The Ohio public records law has a strong underlying policy favoring public access to government-held information.<sup>159</sup> As a result, the privacy exceptions to the Ohio public records law are often interpreted quite narrowly, allowing public access to documents containing personal information in a variety of situations.<sup>160</sup> However, the provision that exempts "[r]ecords the release of which is prohibited by state or federal law"<sup>161</sup> is generally effective in preventing disclosures of personal information when the law in question clearly limits such disclosures.

d. *State EBT and CSE program and welfare-related regulations*

Ohio law creates a specific "right to privacy" for welfare recipients.<sup>162</sup> The provisions of this "right" strictly limit the ability of agencies to disclose a welfare recipient's personal information. Interestingly, Ohio law explicitly states that the " 'right of privacy' means that the individual controls the information held by the [state agency]" and that "[a]ll uses of personal information should be examined with reference to this concept".<sup>163</sup> It is unclear the extent to which this regulation applies to private contractors, but it is likely that they must comply with it as well.

There is an additional privacy provision in the Ohio Administrative Code regarding the interface between a county department of human services (CDHS) and the Child Support Enforcement Agency (CSEA). The public assistance programs and the child support programs both serve to assist families. To help in the sharing of information between these two programs, the Ohio Administrative Code provides that "[t]he applicant's/recipient's right to privacy is safeguarded in the sharing of information between the two separate units. The CDHS is not to prohibit disclosure of relevant information. The CSEA shall be allowed to review the assistance group record when necessary".<sup>164</sup> The two agencies are also required to develop the procedures for a review process.

Information in the Child Support Enforcement system is specifically protected under Ohio Administrative Code section 5101:1-29-071, which states that "[n]o person shall disclose information concerning applicants for and recipients of child support enforcement program services. . . except as provided in this rule." Since the information contained in the new hire data base is provided for the express purpose of locating individuals to establish paternity and for establishing, modifying, and enforcing support

---

<sup>159</sup> Although neither of these phrases is statutorily defined in the Public Records Act, R.C. 149.43 should generally be construed to further broad access, *State ex rel. Cater v. N. Olmsted*, 69 Ohio St.3d 315, 320, 631 N.E.2d 1048, 1053 (1994), and any doubt should be resolved in favor of disclosure of public records.

<sup>160</sup> David S. Jackson, *Privacy and Ohio's Public Record Act*, 26 CAP. U. L. REV. 107, 112 (1997).

<sup>161</sup> OHIO REV. CODE ANN. § 149.43(A)(1)(p).

<sup>162</sup> OHIO ADMIN. CODE § 5101:1-1-03 (1997).

<sup>163</sup> OHIO ADMIN. CODE § 5101:1-1-03(A).

<sup>164</sup> OHIO ADMIN. CODE § 5101:1-3-131(C).

orders and collecting wage information for child support purposes, section 5101:1-29-071 would apply to the information contained in the new hire database.

e. *Contract provisions*

Ohio has used nondisclosure clauses in its contract with the system operator and in its retailer agreements. These clauses have limited the ability of the system operator and the participating retailers to disclose information that they have received while participating in the EBT program. The specific language used was not available in time for this study; however, similar language used in an interagency data-sharing agreement was available.<sup>165</sup> Essentially, this data-sharing agreement requires that the parties adhere to state and federal laws concerning confidentiality, disclose information only as permitted by the agreement, and "specifically agree to comply with state and federal confidentiality laws and regulations applicable to the program(s) under which [the] agreement is funded".

D. TEXAS<sup>166</sup>

**TEXAS EBT FACTS**

<b>Statistics</b>	
Number of Food Stamp Program Households	666, 600 <sup>167</sup>
Number of EBT Households	666, 600 <sup>168</sup>
Number of Authorized Retail Food Stores	13, 545 <sup>169</sup>
<b>Alliance</b>	None <sup>170</sup>
<b>EBT Deployment Status</b>	Statewide <sup>171</sup>
<b>System Operator</b>	Transactive <sup>172</sup>
<b>Administering Agency</b>	Dept. of Human Services

1. *Overview of the state's EBT program*

Texas operates the largest single EBT system in the country, with well over half a million participating households. The Texas EBT card--the Lone Star card--is a magnetic-stripe card issued with a PIN. Of particular interest is the Lone Star Imaging

<sup>165</sup> This agreement is on file with the author.

<sup>166</sup> Texas officials were not available for comment on this study.

<sup>167</sup> ESTIMATED EBT CONTRACTOR ROLL-OUT NUMBERS BY STATE, *supra* note 104, at 3.

<sup>168</sup> *Id.*

<sup>169</sup> FOOD STAMP PROGRAM EBT PROJECT STATUS HIGHLIGHTS, *supra* note 106, at 24.

<sup>170</sup> However, Texas has been cooperating with New Mexico and Oklahoma to allow cross-border EBT transactions among the three states. *Id.* at 24.

<sup>171</sup> *Id.* at 2. Texas reached statewide implementation in November 1995. *Id.* at 24.

<sup>172</sup> *Id.* However, Transactive has ended its EBT operation and is in the process of transferring it to Citibank.

Program, which is intended to replace the PIN with a biometric measurement of each client's fingerprint.<sup>173</sup>

As a condition to participation in the program, Texas requires clients to submit to a finger imaging.<sup>174</sup> The images are stored in a database and are matched up against a scanned fingerprint each time an EBT transaction occurs. The rationale for this is twofold: first, multiple cards and PIN numbers can be fraudulently acquired by one person who supplies false identities. A database of fingerprints makes this much more difficult, since each fingerprint is unique to one person. Second, an EBT card and an associated PIN can be sold in the black market. This, too, is more difficult if the authorized recipient must participate (i.e., must be on hand for the fingerprint verification) in each transaction.

Texas asserts that its system protects the confidentiality of client information. However, the extent to which personal information is available to the system operator and retailer, and whether these parties have any special contractual duties to avoid disclosing such information, is unclear from the published material.

## 2. *Overview of the state's New Hire Directory*

Texas has had a voluntary new hire reporting program since September 1993. In 1995, the Texas Legislature expanded the voluntary program and allowed the Texas Work Force Commission, the Workers' Compensation Commission, and the Department of Human Services to compare the new hire data with their respective databases.<sup>175</sup> The Employer New Hire Reporting Program statute passed in 1995, before the new federal requirements were established. The voluntary reporting statute does not appear to have been repealed, based on research of the available laws. The statute provides for the establishment of reporting procedures for ensuring that employers comply with the federal law.<sup>176</sup> However, the new Texas law establishing the new hire directory is worded in mandatory language, in seeming contradiction to the "voluntary" language used in Texas' original new hire law: "[E]mployers in the state *shall* report each newly hired or rehired employee. . .".<sup>177</sup> Clarifying this a little is information from the web site for the new hire program that indicates that the Employer New Hire Program is currently implemented in Texas on a voluntary basis, but under federal and state law will become mandatory on October 1, 1998.

Whether the program is voluntary or mandatory, Texas law does address the confidentiality of information that is (and will be) contained in the new hire database. The Texas Family Code provides specifically for the protection of confidential information: "All files and records of services provided under this chapter, including

---

<sup>173</sup> *Id.*

<sup>174</sup> TEX. ADMIN. CODE tit. 40, § 3.7001(b) (1998); Colleen Edwards, *The Lone Star Imaging System*, BIOMETRICS IN HUMAN SERVICES USER GROUP NEWSLETTER 2 (vol. 1, issue 4, May 1997) <<http://www.dss.state.ct.us/faq/bhsug04.htm>>.

<sup>175</sup> TEX. FAMILY CODE ANN. § 234.103 (West 1995).

<sup>176</sup> TEX. FAMILY CODE ANN. § 234.104.

<sup>177</sup> TEX. FAMILY CODE ANN. § 234.103 (emphasis added).

information concerning a custodial parent, noncustodial parent, child and an alleged or presumed father, are confidential".<sup>178</sup>

From information obtained from the state's web site, it appears that employers report directly to the state, through the state operations center. No information is available as to the actual implementation of the program, how the agency runs the program, how matching against the child support information is conducted, or whether a third-party contractor provides support.

3. *Selected state legal and regulatory issues*

a. *Informational privacy in the state constitution*

The Texas Constitution does not specifically provide for the protection of informational privacy.

b. *Omnibus privacy act*

Texas does not have an omnibus privacy act.

c. *Public records law*

As with most states, Texas has a strong policy favoring the disclosure of public records.<sup>179</sup> However, also like other states, Texas has set out a number of exceptions to this policy of full disclosure. The most relevant exception is for confidential information: "Information is excepted from the [requirement for disclosure] if it is information considered to be confidential by law, either constitutional, statutory, or by judicial decision".<sup>180</sup> Disclosure of information considered confidential by any person is a criminal offense.<sup>181</sup>

d. *State EBT and CSE program and welfare-related regulations*

Texas has a number of regulations restricting the disclosure of information acquired and used for public assistance programs. These regulations consistently state that the nondisclosure requirements of the relevant federal regulations must be adhered to by the Department of Human Services.<sup>182</sup> The regulations also restrict the sharing of personal information about welfare recipients among state agencies, and they require a written agreement from the requesting agency "that acknowledges compliance with

---

<sup>178</sup> TEX. FAMILY CODE ANN. § 231.108a.

<sup>179</sup> TEX. GOV'T CODE ANN. § 552.001.

<sup>180</sup> TEX. GOV'T CODE ANN. § 552.101.

<sup>181</sup> TEX. GOV'T CODE ANN. § 552.352.

<sup>182</sup> See TEX. ADMIN. CODE tit. 40, § 71.4(a), 71.11(a), 71.12(d), 71.14(b).

state and federal confidentiality requirements".<sup>183</sup> In addition, the regulations extend this requirement to any contractors that will use the information.<sup>184</sup>

Texas also has regulations specifically addressing disclosure of information in its food stamp program. Except primarily for program administration and program-related law enforcement purposes, personal information about clients cannot be disclosed without the client's written permission.<sup>185</sup>

e. *Contract provisions*

The status of the system operator and standard retailer agreements concerning nondisclosure requirements was unavailable at the time of this writing.

E. WASHINGTON

**WASHINGTON EBT FACTS**

<b>Statistics</b>	
Number of Food Stamp Program Households	155, 072 <sup>186</sup>
Number of EBT Households	0 <sup>187</sup>
Number of Authorized Retail Food Stores	3, 291 <sup>188</sup>
<b>Alliance</b>	Western States EBT Alliance <sup>189</sup>
<b>EBT Deployment Status</b>	System operator selected <sup>190</sup>
<b>System Operator</b>	Citibank <sup>191</sup>
<b>Administering Agency</b>	Dept. of Social and Health Services

1. *Overview of the state's EBT program*

Washington has contracted only recently with Citibank, its system processor, to begin deployment of an EBT system.<sup>192</sup> However, many of the details have already been established, although some variance in implementation can be expected. The Washington EBT system will operate over the commercial ATM network, using a magnetic-stripe card/PIN combination. The first pilot phase will begin in early 1999, with statewide implementation slated for the end of 1999.<sup>193</sup>

<sup>183</sup> TEX. ADMIN. CODE tit. 40, § 71.14(b).

<sup>184</sup> TEX. ADMIN. CODE tit. 40, § 71.14(b).

<sup>185</sup> TEX. ADMIN. CODE tit. 40, § 3.3101(a)(1)-(5).

<sup>186</sup> ESTIMATED EBT CONTRACTOR ROLL-OUT NUMBERS BY STATE, *supra* note 104, at 1.

<sup>187</sup> *Id.*

<sup>188</sup> FOOD STAMP PROGRAM EBT PROJECT STATUS HIGHLIGHTS, *supra* note 106, at 26.

<sup>189</sup> *Id.*

<sup>190</sup> *Id.* at 3. Washington's first pilot projects will begin in 1998 or 1999. *Id.* at 26.

<sup>191</sup> Washington is still negotiating a final contract with Citibank. *Id.*

<sup>192</sup> Wash. Dept. of Hum. Services, NEWS IN BRIEF 1 (May 19, 1998).

<sup>193</sup> *Id.*

As currently planned, the system operator will have a significant amount of personal information about each client on file, including name and account balance, as well as other data elements. One of the reasons that Washington has opted for allowing this kind of access to personal information is so the system operator can operate a full-service help desk for the clients.

The retailer in the Washington system is an entirely different matter. The retailer gets no information other than whether the account has sufficient funds to meet the transaction.

## 2. *Overview of the state's New Hire Directory*

Washington had an active new hire directory for eight years prior to the federal national new hire database legislation. In order to meet all of the new criteria set by the federal law, Washington enacted new legislation to establish the new hire directory and to set out the reporting requirements for employers.<sup>194</sup> The new legislation also states that the information can be retained only when "the registry is responsible for establishing, enforcing or collecting a support debt of the employee".<sup>195</sup> The information must be retained long enough to transmit the information to the National Directory of New Hires or to other state agencies, as required by law. The Child Support Enforcement Agency has determined that the timeframe for retention shall be six months, assuming that the employer is in compliance and the information is automatically deleted from the system at the end of the timeframe.

Employers report directly to the Child Support Enforcement Agency, which maintains the new hire database. The new hire information is matched against the Child Support database three times per week. The information in the new hire database is available only to those agencies specified by the law. Although the Washington statute does not, in fact, specify the agencies allowed access to new hire information, it does adopt the restricted agency usage outlined under federal law. In order for an authorized agency to access the data, there only needs to be a formal request from that agency to the Child Support Division; no matching agreement or interagency agreement is required.

The Washington Revised Code also specifically enumerates the appropriate circumstances for the disclosure of records. These circumstances include disclosure to any government agency if (1) the disclosure is necessary for child support enforcement purposes, (2) the disclosure is required under Title IV-D of the federal Social Security Act, (3) the disclosure is necessary for the efficient administration of the support enforcement program, or (4) the disclosure is necessary to the performance of functions and responsibilities of the support registry and the division of child support, as set forth in state and federal statutes.<sup>196</sup>

---

<sup>194</sup> WASH. REV. CODE § 26.23.040 (1997).

<sup>195</sup> WASH. REV. CODE § 26.23.040(7).

<sup>196</sup> WASH. REV. CODE § 26.23.120.

To protect the confidentiality of information obtained through the child support enforcement division (including the new hire database) each employee of the state agency must sign a confidentiality statement when hired and sign a new statement each year thereafter.

Washington uses Connect: Direct to transmit the new hire information to the federal database. Washington reported no known major privacy problems in the operation of its system.

### 3. *Selected state legal and regulatory issues*

#### a. *Informational privacy in the state constitution*

Of the five states that we are studying, only Washington has a constitutional provision specifically protecting privacy: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law".<sup>197</sup> However, as is the case at the federal level, the extension of constitutional protection to informational privacy remains limited.

#### b. *Omnibus privacy act*

Washington does not have an omnibus privacy act.

#### c. *Public records law*

In Washington, the policy behind the public records law strongly favors disclosure.<sup>198</sup> However, there are several significant limitations on this policy when such disclosures may impinge upon personal privacy. First, the Washington public records law includes a general prohibition against disclosures that result in an "invasion of privacy":

A person's "right to privacy," "right of privacy," "privacy," or "personal privacy," as these terms are used in this chapter, is invaded or violated only if disclosure of information about the person: (1) would be highly offensive to a reasonable person, and (2) is not of legitimate concern to the public. The provisions of this chapter dealing with the right

---

<sup>197</sup> WASH. CONST., art. I, § 7. Although every state has a provision similar to the federal Constitution's Fourth Amendment, the use of the phrase "private affairs" in the Washington State Constitution seems to indicate that this section *may* be something more than a reiteration of the federal right. In dicta, the "Washington Supreme Court acknowledged that the state constitution may also protect against compelled disclosure of personal information". Note, *Privacy Rights in State Constitutions: Models for Illinois?* U. ILL. L. REV. 215, 252 (1989) (discussing *Peninsula Counseling Center v. Rahm*, 105 Wash. 2d 929, 719 P.2d 926 (1986)).

<sup>198</sup> WASH. REV. CODE § 42.17.251. "The public records subdivision of this chapter shall be liberally construed and its exemptions narrowly construed to promote this public policy [of keeping the people informed of government activities]."

to privacy in certain public records do not create any right of privacy beyond those rights that are specified in this chapter as express exemptions from the public's right to inspect, examine, or copy public records.<sup>199</sup>

Of course, this provision, by its terms, indicates that an agency must perform a balancing test between the privacy interest and the "legitimate concern" of the public. This "balancing" may limit the effectiveness of the privacy protection, given the strong policy favoring disclosure and the requirement that the invasion of privacy be "highly offensive to a reasonable person".

Second, and more important in practice, are the specific exemptions for "personal and other records" in the public records law. The most important of these exemptions for the purposes of this study is the one that exempts "[p]ersonal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or *welfare recipients*".<sup>200</sup>

While the public records law does not seem to create any specific criminal or civil liability for improper disclosures, Washington law does make it a crime for state officials to intentionally<sup>201</sup> or negligently<sup>202</sup> breach their general duties under state law. This law does not address private individuals who may be involved in an improper disclosure of information. There is criminal liability for individuals who disclose personal records that they acquired for research purposes, but that is a fairly narrow area.<sup>203</sup>

Washington's Administrative Code exempts certain records from disclosure, including records concerning applicants or recipients of child support enforcement activities, to the extent required by 45 C.F.R. section 302.18 or by Washington Revised Code section 26.23.120.<sup>204</sup> Also exempted is office of support enforcement information regarding the location of parents to the extent required by Washington Revised Code section 74.20.280.<sup>205</sup>

*d. State EBT and CSE program and welfare-related regulations*

The Washington laws governing public assistance are quite clear as to the confidentiality of a welfare recipient's personal records:

For the protection of applicants and recipients, the department and the county offices and their respective officers and employees are prohibited, [except for a few limited exceptions], from disclosing the

---

<sup>199</sup> WASH. REV. CODE § 42.17.255.

<sup>200</sup> WASH. REV. CODE § 42.17.310(1)(a).

<sup>201</sup> WASH. REV. CODE § 42.20.080.

<sup>202</sup> WASH. REV. CODE § 42.20.100.

<sup>203</sup> WASH. REV. CODE § 42.48.050.

<sup>204</sup> WASH. ADMIN. CODE § 388-320-220 (6) (1998).

<sup>205</sup> WASH. ADMIN. CODE § 388-320-220 (7).

contents of any records, files, papers and communications, except for purposes directly connected with the administration of the programs of this title.<sup>206</sup>

However, Washington does require county offices to maintain a list of welfare recipients, including the recipients' names, addresses, and the amount that they have received in public assistance.<sup>207</sup> It is not entirely clear whether this list is available to the public, but in any event, Washington law states that "[i]t shall be unlawful. . .for any person. . .to solicit, publish, disclose, receive, make use of, or to authorize, knowingly permit, participate in or acquiesce in the use of any lists or names for commercial or political purposes of any nature".<sup>208</sup>

e. *Contract provisions*

According to officials with Washington's EBT program, both the system operator and standard retailer agreements have clauses that impose a duty not to disclose client information. The contract with Citibank (the system operator) specifically prohibits the disclosure of client information except for specified program administration purposes.<sup>209</sup> In addition, any party that does receive client information must be informed that it, its employees, and its subcontractors must adhere to the confidentiality clauses in the main contract. Furthermore, the state asserts that it shall be indemnified and shall be entitled to injunctive relief for any improper disclosures of personal information.

F. A BRIEF LOOK AT LOCAL AND TRIBAL ISSUES

Although it was our intention to report on specific issues concerning EBT and the Child Support Enforcement databases at the local and tribal levels, our research has shown that, at least for these two programs, there are no significant variations from state and federal law by either type of jurisdiction. This was confirmed by our contact with state officials. However, our research also revealed that other less well-defined programs *could* be affected by ordinances and other local or tribal rulings concerning privacy.

---

<sup>206</sup> WASH. REV. CODE § 74.04.060. This is reiterated specifically for recipients of food stamp benefits in section 74.04.520.

<sup>207</sup> WASH. REV. CODE § 74.04.060.

<sup>208</sup> WASH. REV. CODE § 74.04.060. This is similar to the Kansas law mentioned earlier and suffers the same possibility of being in violation of the First Amendment. See *supra* note 122.

<sup>209</sup> The Contract provisions concerning confidentiality are on file with the author.

## PART III: OBSERVATIONS AND DISCUSSIONS

### I. INTRODUCTION

The primary purpose of this paper is to identify the legal framework for privacy and to examine how the five selected states have dealt with privacy issues in practice. However, this section looks at some of the potential barriers to intergovernmental data-sharing programs and at some of the limitations of the existing laws and practices for protecting privacy. Although the EBT and Child Support Enforcement case studies were central to the development of this report, the observations below extend beyond the case studies to a more general analysis of intergovernmental data-sharing programs.

### II. OBSERVATIONS AND DISCUSSIONS

#### A. LEGAL ISSUES

##### 1. *The current limitations of the federal and state constitutions*

As noted in the first part of this study, the Supreme Court has only recently recognized *any* Constitutional protection of informational privacy. Although there are some indications that this "right" may expand in the future, the current form of the Constitutional right to informational privacy does little to protect personal information collected and used in government programs.

Of the five states that we examined, only Washington even arguably has a constitutional right to informational privacy. However, this right appears to be no more developed than the federal one.

##### 2. *Limitations of the federal Privacy Act*

The Privacy Act is a fairly limited mechanism for the protection of government-held information. First, it applies only to federal agencies, not to states (even states that are executing federal programs are outside the scope of the Act). Second, the safeguards of the Act are largely procedural, not substantive. The Act does not provide sufficient means to actually prevent improper disclosures; in fact, the remedies to an improper disclosure are minimal. Finally, the Privacy Act has significant loopholes in its routine use exception and in the practice of computer matching. The problem has been (and still is) that agencies tend to automatically label uses of data as "routine uses", without actually focusing on whether the use is really a *compatible use*; that is, one that is consistent with the purpose for which the information was collected.

3. *The dominance of the federal program regulations*

In both of the case studies, by far the greatest privacy protections are provided for in the federal program regulations. Each set of regulations contains express limits on when disclosure is permissible. In discussing the issue of privacy protection with state officials, it was clear that their primary concern in the area of privacy was compliance with the federal regulations. The state laws tended to add little to the limits on disclosure, although, as discussed below, they did add some significant penalties for improper disclosures.

4. *Protection of personal information in both case studies may be greater than for most programs*

Each of the programs that we studied deals with some form of what might be called "sensitive" data. In the EBT program, the data is sensitive because of the stigma and "captured audience" status of recipients of public assistance. In the Child Support Enforcement databases, the sensitive data includes wage data and social security numbers--both of which have very specific limitations on how they can be used. As a result, it is reasonable to conclude that the heightened (and largely satisfactory) attention paid to the protection of personal information in these programs is, to some degree, the result of the greater sensitivity of the data in each program. Other data-sharing programs involving less sensitive issues may have much less in the way of privacy protections.

5. *The possible inadequacy of the "program purpose" umbrella*

The case study programs both allow disclosures that are for "program purposes". Although this is a reasonable exception to the general trend toward nondisclosure (after all, if data cannot be used for program purposes, then there can be no program), it does present a disturbing possibility. If the "program purpose" definition is vague or broadly worded (in any program), then the result may be similar to what we see in the routine use exception to the Privacy Act--the exception will limit the usefulness of the rule. To be sure, neither of these programs seems to suffer from this problem; however, it is also true that these programs are not yet fully implemented on a national level.

6. *Violation of the federal program regulations has unclear consequences*

The federal regulations do not clearly set out the penalties and consequences to a state if it does not properly protect personal information. Although there may be a number of ways to accomplish this function (for instance, the federal government could withhold program funds), the deterrent effect is diminished if the penalties are not expressly stated in the regulations. Also, there are not clear penalties for contractors who violate these provisions, nor does injunctive relief appear to be available.

## 7. *State protections are varied--this could affect interoperability*

Each state in this study deals with personal information in a different way. This is not a serious issue in and of itself, because the federal program regulations provide for most of the protections. Nevertheless, it is possible that too much variance in state laws protecting privacy could create substantial barriers to intergovernmental data-sharing programs. This is particularly true when the liability levels for improper disclosures vary significantly, especially when data subjects in one state (but not in another) can enjoin agencies from making certain disclosures.

Although the existence of liability for improper disclosures is an excellent deterrent, the fact that states assign levels of liability that vary from state to state is problematic for programs that operate across state lines. Interoperability is more than an information technology issue--it is also a legal one. If one state's protection of information is much greater than another's, the resulting tension could serve as a barrier to cross-state operations.

This is more evident in the EBT program than in the Child Support Enforcement databases. In the latter, the express purpose of the federal program is to (in effect) combine state databases into one national database. The ability for state law to interfere with interoperability is neutralized by this specific federal mandate.

Another problem with this variability in state treatment of privacy is that states often are not aware of the specific laws and practices of other states--even of neighboring states. This problem is especially acute when federal data-sharing programs are intended to be interoperable among states.

## 8. *The use of contracts to limit disclosures*

Contracts are clearly a major way to limit the improper use of information by any participant in a data-sharing program. Clauses that clearly define when a disclosure is permissible--and when it is not--and that establish penalties for the violation of the clause are particularly effective. Together with clauses that expressly incorporate the relevant state and federal laws and that extend the restrictions to subcontractors, these provisions are possibly the most important tools for limiting the use to which private contractors may put information acquired in a data-sharing program.

## 9. *Self-regulation*

Neither program is developed enough to have much established in the area of self-regulation; however, a number of commentaries--particularly about the EBT program--indicate that self-regulation is likely to play some role in the protection of personal information. The proposed Quest rules<sup>210</sup> that a number of states have adopted already deal with security requirements, and are likely to address privacy issues more specifically as EBT enters its final phase of deployment. Retailers have

---

<sup>210</sup> See *supra* note 68.

also shown some level of self-regulation by limiting their use of information acquired about food stamp recipients in the paper-based system. It is likely that this policy will be expanded in the future.

However, as discussed below, the only effective way to protect information is to keep it from escaping in the first place. If self-regulation is relied upon exclusively, the deterrent effect may not be sufficient to effectively prevent unauthorized disclosures.

#### *10. Public access and the First Amendment as limits on privacy protection*

Although privacy as an individual right (if not a fully recognized Constitutional right) is growing in importance, there is no doubt that it remains secondary to the rights of public access to government records and the freedom of speech. The former interest's enhanced status is made apparent by the construction of public records laws, particularly the Freedom of Information Act. To the extent that privacy can be protected, it must be, but in the rare case where privacy would stand between the public's "right to know" about the activities of government, privacy must always give way to the interest in open government.

Similarly, the First Amendment makes it quite difficult for governments to protect privacy once information "escapes" from the database/program. Within the limits demanded by the interest in public access, governments can prevent disclosures and can punish those who make unauthorized disclosures. However, once government-held information makes its way into the public domain, the First Amendment makes it very hard for government to prevent further uses of that information.

Interestingly, two states in the study do place restrictions that are intended to apply *after* the personal information is made public--the information cannot be used for political or commercial purposes. For a number of reasons, such laws may not survive serious Constitutional challenge. This limitation on post-"escape" penalties dramatically increases the importance of keeping personal information within the protective "walls" of the program. Indeed, if liability can apply to any party in the program with authorized access to personal information, and that liability is great enough to act as a deterrent, there should be few instances of unauthorized disclosure.

#### *11. Overburdensome regulations*

The Federal Parent Locator Service (FPLS) regulates the new hire directory. The FPLS has adopted the requirements of section 6103 of the Internal Revenue Service regulations regarding the safeguarding of information. It is the perception of several states that these regulations were overburdensome because of the record keeping required to ensure the safeguarding of this information. Not only did these states feel that the requirements were overburdensome for the new hire information, but these states did not use the FPLS on a regular basis due to the record-keeping requirements. Their opinion was that the information received was not of a great

enough benefit when weighed against burden of the record-keeping requirements. The value of the information has increased with the addition of the new hire information, so this "balancing" may have different results in the future.

Another possible burden is found in the Privacy Act and in state equivalents. These acts may impose significant burdens on intergovernmental data sharing, particularly by generating additional paperwork requirements and, in some computer matching situations, by requiring independent verification of information *after* a successful match. State privacy acts and federal or state matching agreements may extend these burdens to state and private sector parties.

## 12. *Limitations of privacy exemptions to state public records laws*

In most states (as is true with the federal government), the privacy exemptions to the state's public records law do not mandate *nondisclosure* of personal information, they just free the agency from being *required* to disclose personal information. Of course, it depends on the state whether it has other laws that may further limit the ability of an agency to disclose "private" information. For instance, the Washington Attorney General's Office noted that the privacy exemptions to its public records act "are exemptions, not prohibitions, from disclosure; therefore, to the extent that no person's *right to privacy* would be invaded by disclosure of the information contained in a record, an agency may waive an exemption if it chooses to do so".<sup>211</sup> This would seem to imply an additional balancing of interests. Of course, any federal laws prohibiting disclosure *do*, in effect, mandate nondisclosure. These laws require state compliance and are generally noted expressly in state laws.

### B. ISSUES OF TECHNOLOGY AND PRACTICE

#### 1. *Designing a system to protect personal information*

Along with specific regulatory limitations on the disclosure of personal information, one of the most important methods for protecting privacy in a data-sharing program is to design the system to prevent all unnecessary disclosures. By system, we mean the technical "system" for operating the program (to the extent that it involves the use of personal information) as well as other practical limitations on access and disclosure.

Each state with an existing EBT program designed the program to minimize the amount of personal information available to *any* party--even those authorized by federal regulations to have *greater* access than that allowed. In fact, in more than one state, the system was designed so as to prevent any participant except for the state agency from having enough information to tie any individual to a transaction. Limiting the number of parties with access to personal information is an excellent way to prevent unauthorized disclosures. In addition, if unauthorized disclosures do occur, the state knows that the most likely breach in security is within its own system

---

<sup>211</sup> Wash. Op. Att'y Gen. No. 1 (1980) (emphasis added).

## 2. *Program purpose versus privacy protection*

Despite the good attention given to privacy issues in both programs, the fact remains that the primary focus of the federal government and the states is on achieving the goals of each program. This, of course, is obvious and necessary, but it does highlight a fundamental conflict: privacy protection is a costly and time-consuming process that may often be imposed on the states in the form of an unfunded mandate. As a result, unless the federal government clearly states the importance of privacy in the regulations (as done in both of the programs in this study) and enforces/oversees the protection of privacy, states may lack the incentive (and the resources) to ensure that privacy is actually protected. This is particularly true when the new program may generate substantial cost savings for the state (as in the fraud-reduction savings projected for the use of EBT for food stamp delivery).

## 3. *Information Technology: Friend and foe of privacy*

The use of information technology presents an interesting dichotomy: While information technologies can greatly improve the ability of government to limit access to information, it is also true that information technologies make information much easier to communicate and can create unique vulnerabilities that did not exist in a paper-based system. Clearly, tools like encryption and password protection add security to a database. On the other hand, information technologies allow governments to get much more information about individuals out of data collections than ever conceived of in a paper-based system, which creates in public perception, if not in actual fact, the appearance of an overly informed government. In addition, databases--particularly those accessible off-site--have the potential of being breached, even with advanced security techniques in place. This potential vulnerability could have dire consequences that were also inconceivable in the paper world: an entire database could be copied and communicated to, potentially, a global audience.

Information technology can also create other problems. Perhaps one of the greatest difficulties in converting to "electronic government" is the public fear of "Big Brother"--of too much information about individuals being in the hands of government. This fear has been demonstrated time again, with increasing frequency in recent years. Citizen hostility may arise as new technologies develop, and governments must make sure, when using these technologies, to build in protections that will lessen this fear and hostility.

## 4. *Enforcement of nondisclosure provisions may vary*

Even if a program's regulations clearly limit permissible disclosures of personal information, there still remains the question of to what extent those limits will be enforced. The federal agency administering the program can only provide so much oversight, and the states in question will surely have differing views on the importance of compliance.

## 5. *Confidentiality and security do not equal privacy*

As mentioned in the beginning of this study, providing for security and confidentiality are not entirely equivalent to providing for privacy. The laws and regulations for neither program made this distinction fully clear. As a result, there will likely be some confusion over the interests underlying the security and confidentiality requirements. This also has the effect of subtly altering the focus of oversight and auditing. An auditor may choose to look more at simple system security issues rather than focus on, for example, privacy principles such as transparency and preventing secondary uses.

## 6. *Internal uses of personal information*

Parties with legitimate access to personal information may be tempted to use that information for internal uses. This is possible in many cases because the focus of the "privacy" protections in the program regulations is on establishing limits on disclosures made to *external* parties. The programs studied have narrowed the field for this problem--for instance, only a few government agencies can access information, and only for program purposes. However, even these programs have some gaps. For EBT, the regulations do not completely settle to what extent a contractor or retailer can use information for internal purposes. This may not be that significant of a problem since the Food Stamp Program regulations do require that the personal information be used only for program purposes. Unfortunately, this "program purposes" language is not part of a general federal requirement, and may not play the same role in future programs.

### C. SPECULATIVE ISSUES

#### 1. *Transaction tracking (with EBT)*

The use of EBT as a delivery mechanism for food stamps raises the possibility of transaction tracking--by the government, by the system operator, or by anyone else who may have access to transaction data. Currently, such tracking, at least as far as who is purchasing what items at what times, is not part of the EBT system. However, it is possible that the USDA or a state agency may use this new capability for any one of a number of seemingly legitimate, program-related purposes. This could create a public perception that one of the prices for participation in a public assistance program may be letting the government know where you are, what you are doing, and what you are buying.

#### 2. *Future expansion of data-sharing programs in general*

One problem with the regulatory framework for privacy in the United States is that a new program can be created, or an existing one expanded, to include any number of collections and disclosures of personal information. There is nothing to prevent Congress (or, if within the scope of the enabling legislation, the administering agency) from greatly expanding the number of data elements shared, or the breadth of

the access to the information. For both programs studied, it is possible that each will likely be expanded in scope as it becomes more firmly established. The National Directory of New Hires, as the most current database for wage information, will be a particularly appealing resource for agencies (and, of course, private sector entities will desire access as well).

EBT may also become attractive as an information source because it is the center of a federal effort to deliver multiple benefits across a single system. It is very likely that these different programs will operate through the use of a single shared database.

### 3. *The future of advanced data management techniques*

The mere collection of information is not, in itself, the greatest worry that citizens have. Rather, it is what can be done with that information that triggers concerns. There are already sophisticated techniques for data mining and for correlating data that can give the owner of a relatively small database a surprising amount of useful (and economically valuable) information about data subjects. With advances in these techniques and in new areas such as artificial intelligence, we may witness a day when a great deal about a person can be told from very little. Governments can avoid negative perceptions by building in clearly defined protections against the misuse of data. However, private sector misuse may be more difficult to deal with, and may, in the long run, be the greater perceived threat to personal privacy.

# PART IV: GUIDELINES FOR PROTECTING PRIVACY IN INTERGOVERNMENTAL PROGRAMS

## I. INTRODUCTION

The following items are proposed guidelines for policy makers to use when contemplating new intergovernmental data-sharing programs. These guidelines are based on our observations about the two federal programs, as well as on secondary sources on privacy and on data sharing in practice.

## II. SOME PROPOSED GUIDELINES

### A. DEFINING THE DATA-SHARING PROGRAM

- Clearly define the purpose of the program and the interests being served.
- Identify *all* possible participants in the program, including state, federal, and local agencies as well as private contractors.
- Define and establish the minimum data needed (by every party to the program) to execute the program and serve the identified interests. This should be done for all forms of data, personal and otherwise.
- Determine whether the program, at any foreseeable stage of operation, will need to operate across jurisdictions (usually states).

### B. CONSIDERING THE ROLE OF PERSONAL INFORMATION IN THE PROGRAM

- Consider the issues of *legal* interoperability. If the program may cross jurisdictions, the differences in the ways that the jurisdictions legally and practically protect personal information could create barriers to the smooth execution of the program. Thus, privacy is not just a matter of protecting individual rights, it is also a question of interoperability.
- Specifically identify the personal information that must be collected, stored, used, exchanged, et cetera for the program to function.
- Evaluate the extent that each party with access to any personal information may be able to tie that information to an individual, even when personal identifiers are stripped from the data.
- Determine the legal environment for (1) personal information in general in each relevant jurisdiction and (2) the specific data elements--some kinds of data receive different kinds of legal treatment (e.g., certain medical or wage information receive special protection).
- Identify the degree to which *existing* laws protect the information. Naturally, this will focus on the least common protection--federal protections and any protections that are common among the states.

- Determine how the public feels about the use of the personal information in question--above and beyond the existing legal protection.

#### C. BALANCING COMPETING INTERESTS

- Balance the interests of the data-sharing program (e.g., fraud reduction, cost savings, et cetera) with the privacy interests of any potential data subjects. If the program can operate in a way that minimizes the impact on personal information, that method should be used, to the greatest extent feasible.
- In balancing these interests, policy makers should keep in mind that the public may be willing to trade *some* loss of privacy for a clearly defined benefit, but only if the loss of privacy is clearly necessary. Note that the public's willingness to make this exchange must be assessed before balancing the interests and that the public's perceptions will vary according to the kind of information collected/used.

#### D. DESIGNING THE SYSTEM

- The design of the system will often be the most important way to prevent unauthorized disclosures of personal information. Both the amount of data used in the program and the number of people with access to that data should be minimized.
- To the extent that state or local governments design their own systems, the federal administering agency should make the preceding point clear in the program regulations.
- Technology that provides additional security for personal information should be used, whenever feasible.

#### E. CONSTRUCTING A PROGRAM-SPECIFIC REGULATORY FRAMEWORK FOR PRIVACY

- Program regulations are the center of any federally-initiated/state implemented program.
- A systematic, well-defined framework for privacy should be developed and set out in an independent section of the program regulations. These regulations should be consistent with existing laws (federal and state), but when they are not, the contradictions should be identified and communicated to the appropriate jurisdictions. If preemption is intended, the federal agency should state so in express language. Remember, too, that contradictory state laws may interfere with the interoperability of a data-sharing program.
- Fair information practices<sup>212</sup> should be the keystone of any regulations dealing with the protection of personal information:
  - 1) Openness. There must be no personal data record-keeping systems whose very existence is secret;

---

<sup>212</sup> U.S. Dep't of Health, Education, and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens 41 (Washington, D.C.: Government Printing Office, 1973) (cited in 1974 U.S.C.C.A.N. 6916, 6923-24).

- 2) Disclosure. There must be a way for an individual to find out what information about him is in a record and how it is used;
- 3) Secondary use. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent;
- 4) Opportunity to amend. There must be a way for an individual to correct or amend a record of identifiable information about him; and
- 5) Security. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

- Specific regulations should be issued addressing each of these fair information practices. They should not just be mentioned in the regulations as goals.
- Of these fair information practices, the most important--and the hardest to ensure compliance with--is the prohibition against secondary uses that occur without the data subject's consent.
- The regulations should clearly state when disclosures, uses, et cetera are permissible for each and every participant in the program. Defining permissible disclosures is more effective than defining impermissible ones.
- The regulations should provide the data subjects with an opportunity to review and amend their records.
- The regulations should establish liability and remedies for improper uses, disclosures, et cetera of personal information by any party. Criminal, civil, and injunctive relief should be made available to data subjects. Liability is a critical part of the process--in most cases, if the information "escapes" the system, the government will be unable to make it secret again or to punish those who use it afterwards (due to open government and First Amendment interests).
- The Privacy Act should not be relied upon to protect personal information, even to the extent that it applies at all (i.e., it only applies to the records collected by federal agencies). As noted in Part III of this study, the Privacy Act lacks significant substantive protections of privacy--it focuses primarily on procedural protections. In addition, there is a significant concern that the routine use and computer matching exceptions to the Privacy Act have severely limited the Act's effectiveness at limiting the flow of information.
- Similarly, the Privacy Act should not serve as a model for the federal program regulations. Such regulations should focus on substantive protections, minimizing the paperwork burden of compliance, while maximizing the actual protection of personal information.
- The regulations should address the need for contract clauses that extend the privacy protections to third parties. Model clauses may be included, either in the regulations or in a separate form. Such clauses should incorporate by reference the privacy protections of the state and federal regulations, as well as clear penalties for their violation. In addition, the contract clauses should impose the same standards on any subcontractors.
- The state should be held ultimately responsible for the protection of privacy and for performing audits (of system security *and* of privacy).

#### F. EDUCATING PARTICIPANTS AND DATA SUBJECTS

- Provide participants in the operation of the program with guidance on privacy and security (as two separate, but related, issues).
- Provide data subjects with guidance on their rights.
- Consider the use of a web site to aid in the education of operational participants and data subjects.

#### G. DEVELOPING AND USING A STATE CLEARINGHOUSE

- In major programs that will be operated by a number of states, an on-line clearinghouse should be considered as a method for providing information about how each state is planning, deploying, and operating the program. Through the use of such a clearinghouse, state, federal, and local policy makers can (1) identify best practices, (2) avoid mistakes or problems encountered by other states, and (3) identify different laws, practices, and system designs that need to be harmonized to achieve interoperability (both legal and technical).
- The clearinghouse should be located at the administering federal agency's web site, but persons in each state should be responsible for providing information for the various categories tracked by the clearinghouse.<sup>213</sup>

#### H. AUDITING AND OVERSEEING PRIVACY PROTECTION PRACTICES

- Along with audits for system security, programs should also be audited specifically for compliance with the privacy/nondisclosure provisions of the program regulations.

#### I. PLANNING FOR ANY FUTURE EXPANSION OF THE PROGRAM

- Require full review of any proposed expansion of (1) the amount of personal information collected or (2) access to personal information used in the program.
- The Fair Information Practices and the determinations made originally in the steps above should be revisited when considering expansion of the program in any way. In particular, secondary uses should not be permitted. If a proposed new disclosure or an expanded access to personal information does not serve a primary purpose of the program, it cannot counterbalance the interest an individual has in keeping information about him private.

---

<sup>213</sup> The NSF-funded States Inventory Project (<http://www.states.org/>) is an example of this methodology.