CONFIDENTIALITY OF DOMESTIC VIOLENCE VICTIMS' ADDRESSES

Prepared by the
National Criminal Justice Association

November 1995
A NOTE ON STYLE: For the sake of convenience and consistency, "he," "his," and "him" are used throughout this report to refer to both males and females.
FOREWORD

Passage of the Violence Against Women Act, as part of the Violent Crime Control and Law Enforcement Act of 1994, marked a significant change in our national response to crimes such as domestic violence, sexual assault and stalking. In addition to tough new federal penalties, the Act provides additional resources for the states to hire and train police, prosecutors and victim advocates.

The Act also directed the Attorney General to conduct a study of the various means by which personal information of victims of domestic violence, sexual abuse and stalking becomes publicly available. Congress called on the Attorney General to explore the feasibility of developing protective mechanisms to safeguard confidential information concerning the location or address of victims of abuse.

The safety and security of victims of domestic violence, sexual assault and stalking can be at risk when information about the location of their residence or workplace becomes known by their victimizer. The act of leaving a relationship can invite a violent and, in some cases, a deadly response from an abusive partner. In such situations, a secure address becomes all the more crucial. Victims of sexual assault may require absolute confidence in their privacy in order to assure their emotional recovery and physical safety. Finally, a stalking victim who takes steps to block access to private information should be entitled to just that - control of access to her personal information.

This report represents a first step toward addressing these problems and is the result of a collaboration by representatives from private corporations, domestic violence advocacy organizations, nonprofit service groups, and government agencies among others. It reveals that information pertaining to the location of victims of violence is readily available through a variety of legitimate means. Postal services, voter registration records, motor vehicle records, school records, credit bureaus, computerized data bases, and caller ID are all sources of critical information that might, in the wrong hands, lead to further abuse and criminal actions.

The report highlights the importance of balancing the confidentiality of personal information of victims against the importance of providing public access to address information for legitimate purposes and in compliance with constitutional constraints. It recommends education as the primary tool to accommodate that balance. Employees handling personal information need a greater understanding of privacy rights. Victims of violence must be made aware both of the technology which compromises their security, and the services and options which may help guard confidential information about themselves.

However, enhanced understanding of privacy is only a small part of ensuring that victims of violence can reclaim a sense of peace and security in their lives. The report also recommends that states should reevaluate their privacy and confidentiality statutes to determine their effectiveness. Public agencies should seek to adopt or improve internal protocols which govern the dissemination of personal information. Private companies should examine their procedures surrounding the confidentiality and possible disclosure of information which may place victims and their families at risk. The impact of the Internet and related technological developments needs to be addressed.

The Justice Department is committed to assisting in the national effort to address the difficulties encountered by Americans facing the continued threat of violence. This report should serve as a resource for further investigation and action.

Bonnie Campbell
Director, Violence Against Women Office
PREFACE

The threat of injury or death is a constant in many domestic violence victims' lives. For many of these victims, relocation may become a necessary step in their quest for safety for themselves and, oftentimes, for their children.

But relocation may not ensure the domestic violence victim’s safety for very long. With the deliberate, unknowing, or inadvertent cooperation of friends, relatives, and colleagues, the batterer may be able to secure information that will lead him to his victim. Numerous public agencies, such as state motor vehicle departments, and private organizations, such as credit bureaus, operate data sources that contain information about the domestic violence victim. The batterer may have legitimate access to these systems or, with the help of an unscrupulous associate, gain access illegally.

The Congress' call for a study of the means by which abusive spouses obtain information about the locations of their spouses reflects contemporary concern about this critical aspect of the plight of domestic violence victims. The Congress directed the U. S. attorney general to report on these means and an analysis of the feasibility of creating effective measures for protecting the confidentiality of information concerning the locations of abused spouses.

Research carried out for the project identified myriad sources of information that could be used by a batterer to locate his victim; indicated a need to learn more about which potential information sources batterers use most frequently to locate their victims' addresses; and underscored the need for more education in the public and private sector and of victims on confidentiality issues as they relate to domestic violence victims and ways to prevent unwanted disclosures.

Preventing the batterer from inflicting further violence on his victim is at the heart of strategies to intervene effectively in domestic violence. This important public safety objective should be addressed through appropriate actions in the public and private sectors to support a domestic violence victim’s decision to relocate and withhold his location from the batterer. We hope that information developed through this study will contribute to such improvements.

Gwen A. Holden
Executive Vice President
National Criminal Justice Association
RESOURCE GROUP BIOGRAPHIES

The National Criminal Justice Association (NCJA) gratefully acknowledges the contributions of the following individuals who gave generously of their time and talents.

Project Resource Group:

AILEEN ADAMS. Ms. Adams is the director of the U. S. Department of Justice’s Office for Victims of Crime (OVC). Prior to assuming that position, Ms. Adams served as legal counsel for the Rape Treatment Center at the Santa Monica (Calif.) Hospital Medical Center and founded the Stuart House, a program for sexually abused children. She has worked as a prosecutor, police reserve officer, probation officer, and legal advocate for crime victims. Ms. Adams received a bachelor of arts degree from Smith College (Mass.) and a Juris Doctor from Howard University (D. C.).

AMY V. ANDERSON. Ms. Anderson is assistant manager for corporate assurance performance for the Bell Atlantic Corporation (Bell). Prior to accepting that position, she held several other positions with the company, including assistant manager for privacy and public policy. Ms. Anderson received a bachelor of science degree from the University of Maryland.

BERNARD V. AUCHTER. Mr. Auchter is a program manager for the U. S. Department of Justice, National Institute of Justice (NIJ), where he manages the Family Violence Research Program. He has served the NIJ in a variety of capacities since 1975. He received a bachelor of arts degree from Villanova University (Pa.) and a master of social work degree from Rutgers University (N. J.).

DAVID BEATTY. Mr. Beatty currently is the director of public policy at the National Victim Center (NVC), where he is responsible for all matters related to legislative and legal issues regarding victims’ rights and interests. Mr. Beatty also serves as director of the NVC’s Crime Victim Litigation Project and the Coalition of Victims’ Attorneys and Consultants. He currently serves on the Victim Committee of the American Bar Association and is a member of the American Restitution Association and the National Constitutional Amendment Network. Mr. Beatty received a bachelor of arts degree in political science from Colorado College and a Juris Doctor from the University of Iowa School of Law.

JOHN P. BENDER. Mr. Bender is the senior deputy attorney general in charge of administrative agency advice for the New Jersey Department of Law and Public Safety’s Division of Law. He has served in the Division of Law in a variety of capacities since 1982. He received a bachelor of arts degree from Boston College (Mass.), a master of arts degree from Fordham University (N. Y.), and a Juris Doctor from Seton Hall Law School (N. J.).

JERRY CERASALE. Mr. Cerasale is senior vice president for government affairs for the Direct Marketing Association (DMA). Prior to joining the DMA, he served as the deputy general counsel for the U. S. House of Representatives’ Committee on the Post Office and Civil Service, and in several capacities at the Postal Rate Commission and the U. S. Postal Service. He received a bachelor of arts degree from Wesleyan University (Conn.) and a Juris Doctor from the University of Virginia School of Law.

LORNA CHRISTIE. Ms. Christie is the vice president of consumer affairs for the Direct Marketing Association (DMA), where she is responsible for the self-regulatory and public affairs programs. In January 1992, she left the DMA to serve as the associate director for business affairs for the U. S. Office of
Consumer Affairs. She returned to the DMA in the fall of 1992 to direct the Privacy Task Force. Ms.
Christie received a bachelor’s degree from East Carolina University (N. C.).

**DAN M. EDDY.** Mr. Eddy is the executive director of the National Association of Crime Victim
Compensation Boards. Previously, Mr. Eddy directed the Crime Victim Project for the National
Association of Attorneys General and worked as an attorney in private practice. He received a bachelor of
arts degree from Harvard University (Mass.) and a Juris Doctor from the University of Maryland.

**ROBERT A. FEIN.** Mr. Fein is a forensic psychologist who currently is a visiting fellow of the U. S.
Department of Justice, National Institute of Justice and a consultant psychologist with the U. S.
Department of the Treasury’s U. S. Secret Service. He co-directs the Secret Service Exceptional Case
Study Project, a multi-year operational study of violence directed at public officials and public figures.
Previously, Mr. Fein worked for 15 years as a clinical and forensic psychologist with mentally disordered
offenders in Massachusetts and with the mental health and correctional systems that evaluate and care for
them. He received a bachelor’s degree in American studies from Amherst College (Mass.) and a doctorate
degree in clinical psychology and public practice from Harvard University (Mass.).

**JON R. FELDE.** Mr. Felde is general counsel of the National Conference of State Legislatures (NCSL)
and director of the NCSL’s Committee on Law and Justice. Prior to joining the NCSL in 1986, he
practiced law in Franklin, Ky., with the firm of Harlin, Parker & Rudloff. Mr. Felde received a bachelor of
arts degree from Harvard University (Mass.) and a Juris Doctor from the University of Kentucky College
of Law.

**CARMAN A. GANNOTTI.** Mr. Gannotti is the director of the U. S. Department of the Treasury,
Internal Revenue Service’s (IRS) Office of Disclosure, which administers compliance with the IRS’
confidentiality statute, the Privacy Act, and the Freedom of Information Act. Mr. Gannotti has served at
the IRS in a variety of capacities since 1964. He received a bachelor of science degree from Villanova
University (Pa.).

**DONALD HAINES.** Mr. Haines is legislative counsel for the American Civil Liberties Union (ACLU),
where he handles issues concerning personal privacy, cyberspace, the information infrastructure, and
workplace rights. Prior to joining the ACLU, Mr. Haines served as a legislative attorney for the
Congressional Research Service and the American Federation of Government Employees. He received a
bachelor of arts degree from Harvard University (Mass.) and a Juris Doctor from the University of Virginia
School of Law.

**SUSAN W. HILLENBRAND.** Ms. Hillenbrand has worked for the American Bar Association (ABA) for
more than 20 years and currently is director for special projects for the ABA’s Section for Criminal Justice.
During her tenure, Ms. Hillenbrand has contributed to a variety of victim assistance research projects and
publications. She also has served as a consultant to the National College of the Judiciary and as a
contractor for the U. S. Department of Labor, Office of the Assistant Secretary for Policy, Evaluation, and
Research. Ms. Hillenbrand received a bachelor’s degree in political science from Marymount College
(N.Y.) and a certificate from the Paralegal Institute (N.Y.).

**NOLAN E. JONES.** Mr. Jones is the director for the Human Resources Group of the National
Governors’ Association (NGA). He has served as staff director for the NGA’s Committee on Justice and
Public Safety. Previously, Mr. Jones was assistant professor of political science at the University of
Michigan in Ann Arbor. Recently, he was elected to the governing council of the American Political
Science Association. He received an undergraduate degree from Texas Southern University and a doctoral degree in political science from Washington University (Mo.).

SUSAN KEILITZ. Ms. Keilitz is a senior research associate at the National Center for State Courts, where she directs a study of effective court practices for custody cases that involve domestic violence and a study of the use of civil protective orders to deter domestic violence. She received a bachelor of arts degree from Indiana University (Ind.), a master of education degree from Arizona State University, and a Juris Doctor from the College of William and Mary's Marshall-Wythe School of Law (Va.).

DAVID S. KIERNAN. Mr. Kiernan is director of federal government relations for Associated Credit Bureaus, Inc. (ACB). Prior to joining ACB, Mr. Kiernan operated a lobbying and consulting firm, served as deputy director of congressional relations for the Office of Thrift Supervision and the Federal Home Loan Bank Board, and held a number of positions with members of the U. S. Congress. He attended the U. S. Naval Academy (Md.) and received a bachelor of arts degree from Johns Hopkins University (Md.). He also attended Boston College School of Law (Mass.).

JENNIFER KNOBE. Ms. Knobe is a grant program specialist for the U. S. Department of Justice, Bureau of Justice Assistance (BJA). Previously, she was a research intern at the American Prosecutors Research Institute. Ms. Knobe presently is pursuing a master’s degree in public administration, with a concentration in judicial management in public organizations, at George Washington University (D. C.). She received a bachelor’s degree in criminal justice from State University of New York at Albany.

JOHN C. LANE. Lt. Lane is a 23-year veteran of the Los Angeles (Calif.) Police Department and serves as the officer in charge of the department’s Threat Management Unit, which focuses on abnormal, long-term threat and harassment cases. Lt. Lane is the founder and current president of the Association of Threat Assessment Professionals. He received a bachelor’s degree in physical education from California State University at Long Beach and a master’s degree in public administration from University of Southern California.

NORMA MANCINI STEVENS. Ms. Stevens is a senior policy analyst with the American Prosecutors Research Institute, where she coordinates two U. S. Department of Justice-funded projects on domestic violence and stalking and violence against women. Previously, she served as chief of the Justice Department’s Bureau of Justice Statistics (BJS), Fiscal and Management Division. As a presidential management intern for the federal government, she served in the Justice Department’s U. S. Marshals Service, on the U. S. Senate Judiciary Committee staff, and in the BJS. Ms. Stevens received an undergraduate degree from Lake Erie College (Ohio) and a master’s degree in public administration from George Washington University (D. C.).

ANNE E. MENARD. Ms. Menard is the director of the National Resource Center on Domestic Violence, a U. S. Department of Health and Human Services-funded project of the Pennsylvania Coalition Against Domestic Violence. Previously, she served as director of the Office of Victim Services of the Connecticut Judicial Branch and executive director of the Connecticut Coalition Against Domestic Violence. She received a bachelor of arts degree from Colby College (Maine).

LOIS F. MOCK. Ms. Mock has been at the U. S. Department of Justice’s National Institute of Justice (NIJ) since 1972. She presently serves as a program manager in the NIJ’s Office of Research and Evaluation. Ms. Mock received an undergraduate degree from Oberlin College (Ohio) and a master’s degree in social psychology from the University of Michigan.
CATHERINE PIERCE. Ms. Pierce is a policy specialist in the U. S. Department of Justice’s Violence Against Women Grants Office. Previously, she served as director for the Summer of Safety Grants Program at the Corporation for National Service, senior program officer at the State Justice Institute, and in a variety of positions for community service projects. She received a bachelor of education degree from the University of Massachusetts.

ROXANN M. RYAN. Ms. Ryan is an assistant attorney general of Iowa in the Criminal Appeals Division. She has worked in the Iowa Attorney General’s Office since 1980, previously serving as deputy attorney general, division head, and staff attorney in the Criminal Appeals Division. Ms. Ryan is a full-time student in the criminal justice doctoral program at the University of Nebraska at Omaha. Ms. Ryan received a bachelor’s degree in economics and a Juris Doctor from Iowa State University.

ALDEN SCHACHER. Ms. Schacher is government relations manager for the Information Industry Association. Previously she served as a legislative assistant for former Rep. Dave McCurdy (D-Okla.). She received a bachelor of science degree from Oklahoma State University.

JOHN H. STEIN. Mr. Stein has been deputy director of the National Organization for Victim Assistance (NOVA) since 1981. Previously, he served as vice president of the NOVA Board of Directors. Mr. Stein’s experience in victim services has included helping to train an experimental team of community service officers in the Dayton (Ohio) Police Department and designing paralegal roles for the U. S. attorney’s office in Washington, D. C. He also served as deputy director of the Criminal Justice and the Elderly Project at the National Council of Senior Citizens, where he helped design service programs for elderly crime victims and provided technical assistance to elderly crime projects across the nation. Mr. Stein received a bachelor’s degree from Yale College (Conn.) and a Juris Doctor from George Washington University (D. C.).

ROBERT N. VEEDE. Mr. Veeder is the privacy advocate for the U. S. Department of the Treasury’s Internal Revenue Service (IRS). In this capacity, he is responsible for fostering understanding of the public’s rights regarding information provided to the IRS and developing and conducting privacy training for the agency. Previously, Mr. Veeder served as a senior policy analyst in the Office of Management and Budget. He is an instructor at the U. S. Department of Agriculture’s graduate school and the U. S. Department of Justice’s Legal Education Institute on privacy issues. He received a bachelor of arts degree from Yale University (Conn.) and a master’s degree in public administration from the American University (D. C.).

ALBERT A. VERVILLE. Mr. Verville is coordinator of central registration for the Fairfax County (Va.) Public Schools. He previously served as a specialist in English as a second language and a teacher for the county. He received a bachelor of arts degree from the University of Maine, a master of arts degree from Middlebury College (Vt.), and a doctor of education degree from Vanderbilt University’s George Peabody College (Tenn.).

BRIAN VOSSEKUIL. Mr. Vossekuil is a special agent of the U. S. Department of the Treasury’s U. S. Secret Service, where he serves as assistant special agent in charge of the Domestic Investigations Branch of the Office of Protective Research. Mr. Vossekuil codirects the Secret Service Exceptional Case Study Project, a multi-year operational study of violence directed at public officials and public figures. During his 17-year career with the Secret Service, Mr. Vossekuil has served in the Detroit, Mich., field office; in the Presidential Protective Division; and in the Intelligence Division. Mr. Vossekuil received a bachelor of arts degree from Kalamazoo College (Mich.).
JOAN C. WEISS. Ms. Weiss is the executive director of the Justice Research and Statistics Association (JRSA). Previously, she served as the executive director of the National Institute Against Prejudice and Violence and as a community relations specialist for the Montgomery County (Md.) Human Relations Commission. She received a bachelor of science degree in sociology and a master of social work from the University of Maryland.

Attendees:

BARBARA HART. Ms. Hart is legal director for the Pennsylvania Coalition Against Domestic Violence, associate director of the Battered Women’s Justice Project, and legal consultant to the National Resource Center on Domestic Violence. She also has a private practice, which focuses on consultation and training in domestic violence issues. She received a bachelor of arts degree from the University of Michigan and a Juris Doctor from George Washington University (D.C.).

NANCY A. TURNER. Ms. Turner is the public policy advocate for the National Coalition Against Domestic Violence and a program coordinator for a nonprofit shelter in Arlington (Va.). She also teaches a course on women and violence at George Washington University (D.C.). Ms. Turner received a bachelor of science degree from the University of Connecticut and master of arts in women’s studies and public policy from George Washington University (D.C.).

Project Staff:

Gwen A. Holden, executive vice president, National Criminal Justice Association (NCJA)
Paul E. Lawrence, director of administration and information systems, NCJA
Lisa Doyle Moran, assistant director for legal affairs, NCJA
Robert A. Kapler, senior staff associate, NCJA
Patrick M. Meacham, senior staff associate, NCJA
Nadine M. Rapacioli, staff attorney, NCJA
Carolyn J. Reid, administrative assistant, NCJA
Jennifer A. Ferrante, legal researcher, NCJA
Robert L. Goldstein, former legal researcher, NCJA
Amy K. Phillips, former legal researcher, NCJA
D. Brenner Brown, former graduate intern, NCJA
Stacey L. Gosnell, former intern, NCJA
Karen E. Stauss, former intern, NCJA
ACKNOWLEDGEMENTS

The final report for the Project to Conduct a Study Relating to the Confidentiality of Addresses of Victims of Domestic Violence reflects the skills and hard work of the project staff, resource group, and consultants, as well as numerous state, local, and federal officials from whose knowledge and experience the project benefited greatly.

The U. S. Department of Justice, National Institute of Justice (NIJ) project monitor, Bernard V. Auchter, provided valuable guidance and practical advice on issues related to this project.

The NCJA is particularly indebted to the dedicated members of the project resource group: Aileen Adams, director, Office for Victims of Crime, U. S. Department of Justice (OVC); Amy V. Anderson, assistant manager for corporate assurance performance, Bell Atlantic Corporation; David Beatty, director of public policy, the National Victim Center; John P. Bender, senior deputy attorney general, Division of Law, New Jersey Department of Law and Public Safety; Jerry Cerasale, senior vice president, Direct Marketing Association (DMA); Lorna Christie, vice president for consumer affairs, DMA; Dan M. Eddy, executive director, National Association of Crime Victim Compensation Boards; Robert A. Fein, visiting fellow, NIJ, consultant psychologist, U. S. Secret Service, U. S. Department of the Treasury; Jon R. Felde, general counsel, National Conference of State Legislatures (NCSL); Carman A. Gannotti, director, Office of Disclosure, Internal Revenue Service, U. S. Department of the Treasury (IRS); Donald Haines, legislative counsel, American Civil Liberties Union (ACLU); Susan W. Hillenbrand, director for special projects, Section for Criminal Justice, American Bar Association (ABA); Nolan E. Jones, director, Human Resources Group, National Governors' Association (NGA); Susan Keilitz, senior research associate, National Center for State Courts (NCSC); David S. Kiernan, director of federal government relations, Associated Credit Bureaus, Inc. (ACB); Jennifer Knobe, grant program specialist, Bureau of Justice Assistance, U. S. Department of Justice (BJA); John C. Lane, lieutenant, Los Angeles (Calif.) Police Department; Norma Mancini Stevens, senior policy analyst, American Prosecutors Research Institutes (APRI); Anne E. Menard, director, National Resource Center on Domestic Violence; Lois F. Mock, program manager, NIJ; Catherine Pierce, policy specialist, Violence Against Women Grants Office, U. S. Department of Justice; Roxann M. Ryan, assistant attorney general, Office of the Iowa Attorney General; Alden Schacher, government relations manager, Information Industry Association (IIA); John H. Stein, deputy director, National Organization for Victim Assistance (NOVA); Robert N. Veeder, privacy advocate, IRS; Albert A. Verville, coordinator of central registration, Fairfax County (Va.) Public Schools; Brian Vossekuil, assistant special agent in charge, Domestic Investigations Branch, Office of Protective Research, Secret Service; and Joan C. Weiss, executive director, Justice Research and Statistics Association (JRSA).

Project staff also benefitted greatly from the insight and research assistance provided by Barbara Hart, legal director, Pennsylvania Coalition Against Domestic Violence; associate director, Battered Women's Justice project, legal consultant, National Resource Center on Domestic Violence; and Nancy A. Turner, public policy advocate, National Coalition Against Domestic Violence.

Project staff appreciates the time and effort of the domestic violence coalitions that responded to a survey designed to obtain information about difficulties encountered in maintaining the confidentiality of domestic violence victims' locations and recommendations for further action. A list of the responding coalitions is provided in Appendix C.
The project staff also is grateful to the following representatives from the address management unit of the U. S. Postal Service: Michael Selnick and Rocky Matthews. In addition, the following individuals provided the project staff with information on their services: Eric N. Lamb, account representative, WESTLAW; and Christine Kalodikis, customer education support consultant, LEXIS/NEXIS.

Jennifer A. Ferrante, NCJA legal researcher; Robert L. Goldstein, former NCJA legal researcher; and D. Brenner Brown, former NCJA intern; provided valuable support to the research and preparation of this report.

Finally, the NCJA would like to acknowledge the work of the following staff members: Paul E. Lawrence, director of administration and information systems; Lisa Doyle Moran, assistant director for legal affairs; Robert A. Kapler, senior staff associate; Patrick M. Meacham, senior staff associate; Nadine M. Rapacioli, staff attorney; and Carolyn Reid, administrative assistant.
# TABLE OF CONTENTS

## CHAPTER I: INTRODUCTION
- Methodology .......................................................... 3
- Principles that Guided Development of the Report ............. 4
- Definitions and Scope of the Report .............................. 5

## CHAPTER II: CURRENT PRACTICES IN THE PUBLIC SECTOR
- Introduction ............................................................. 7
- Federal Statutes and Policies ........................................ 7
  - Freedom of Information Act and Privacy Act .................. 8
  - Driver Privacy Protection Act ...................................... 9
  - Family Violence Prevention and Services Act and Victims of Crime Act ............. 10
  - Family Educational Rights and Privacy Act ..................... 10
  - Postal Regulations .................................................. 11
  - Internal Revenue Service Policies ............................... 13
    - Statutory Authority ............................................... 13
    - Ensuring Compliance ............................................. 13
    - Relationship to Other Agencies ............................... 14
    - Sanctions .................................................................. 14
- State and Local Confidentiality Policies and Statutes ......... 15
  - General Public Records ......................................... 15
  - Motor Vehicle Records .......................................... 17
  - Voter Registration Records ..................................... 19
  - Legislation to Protect the Privacy of Crime Victims ......... 21
  - School District Policies .......................................... 22
- Selected Case Law Addressing Confidentiality of Address Information ........................................ 23
  - Voter Registration .................................................. 23
  - Motor Vehicle Records ........................................... 25
  - Access for Commercial or Fund-Raising Purposes .......... 27
  - Student Information ................................................ 28
  - Rights of the Media ............................................... 32
- Resource Group Discussion and Recommendations ............. 34
  - Rights of Crime Victims ......................................... 34
  - Statutes, Regulations and Public Policies ...................... 34

## CHAPTER III: CURRENT PRACTICES IN THE PRIVATE SECTOR
- Bell Atlantic Corporation's Privacy Policies .................... 37
  - Use of Information .................................................. 38
  - Security ............................................................... 38
  - Caller ID .............................................................. 39
- Direct Marketing Practices ......................................... 40
  - Use of Information .................................................. 40
  - Guidelines and Policies ......................................... 40
- Credit Bureau Policies .............................................. 41
- Information Industry Association Guidelines ................... 42
CHAPTER I

INTRODUCTION

Domestic violence has become one of the most serious and complex problems facing this nation's criminal justice and social services communities. According to a guide developed by the Urban Institute and the National Council on Juvenile and Family Court Judges, more than 25 percent of married American couples experience one or more incidents of domestic violence, and each year approximately 2 million women are severely assaulted by male partners. In the face of an alarming number of incidents of severe violence against intimate partners, state and federal legislators have passed laws that are intended to hold batterers accountable for their actions and to better protect victims of domestic abuse. This legislation has been informed by an understanding of the behavioral patterns associated with domestic violence and has mandated that law enforcement, prosecutors, and the courts assume more aggressive roles in intervening to end abusive behavior.

According to experts in the field of domestic violence, batterers make persistent attempts to control their intimate partners, following them from home to home, and work place to work place. Batterers frequently are not deterred by court orders to stay away from their victims and repeatedly make efforts to intimidate and harass.

Moreover, studies have shown that a batterer's pursuit of his victim increases when the victim separates from the abuser. The U. S. Department of Justice reported, for example, that women who are divorced or separated are at higher risk of assault than married women. Consequently, providing domestic

---


violence victims the opportunity and means to remove themselves from the threat of further violence has become a principal component of domestic violence reduction strategies.

However, problems in achieving a safe and secure separation of victim and abuser have been compounded by difficulties in keeping information about the victim's location from the abuser. Advances in technology have given batterers easier access to information that may help them locate their victims. In addition, victims often find it difficult to place themselves beyond the reach of abusive partners with whom they have friends or children in common and who know the victims' activities and places of employment.

Responding to evolving concerns about domestic violence victims' safety, the Congress, in the Violent Crime Control and Law Enforcement Act of 1994, directed the U.S. attorney general to conduct a study of the means by which abusive spouses obtain information about the locations of their spouses. The attorney general assigned the responsibility for the study to the U.S. Department of Justice, National Institute of Justice (NIJ), and the NIJ entered into an agreement with the National Criminal Justice Association (NCJA) to manage the project.

Specifically, the Congress mandated that:

(a) REPORT -- The Attorney General shall conduct a study of the means by which abusive spouses may obtain information concerning the addresses or locations of estranged or former spouses, notwithstanding the desire of the victims to have such information withheld to avoid further exposure to abuse. Based on the study, the Attorney General shall transmit a report to the Congress including --

(1) the findings of the study concerning the means by which information concerning the addresses or locations of abused spouses may be obtained by abusers; and

(2) analysis of the feasibility of creating effective means of protecting the confidentiality of information concerning the addresses and locations of abused spouses to protect such persons from exposure to further abuse while preserving access to such information for legitimate purposes.4

The information in this report is intended to guide the Congress and state legislators and policymakers in their debates on these issues. This chapter contains an introduction to the project, which explains the congressional mandate, the project staff's methodology in compiling the report, and the

---

3 Pub. L. 103-322, §40508.

4 Id.
principles that guided report development. Chapter II contains an overview of current practices in the public sector affecting privacy issues, and the resource group's discussion of these issues. Chapter III addresses privacy issues that the private sector has confronted, as well as a summary of the resource group's discussion in this area. Chapter IV summarizes the results of an informal survey on confidentiality issues that was sent to domestic violence coalitions in each state. In Chapter V, the project staff summarized its findings. The appendices contain resource group materials, a copy of the survey, and a bibliography.

Methodology

The project was carried out by the NCJA under the direction and oversight of an NIJ project monitor. The NCJA project staff was assisted in its work by a resource group composed of individuals representing the following organizations and agencies: the Associated Credit Bureau; the American Bar Association; the American Civil Liberties Union; the Bell Atlantic Corporation; the Direct Marketing Association; the Fairfax County (Va.) Public Schools; the Information Industry Association; the Iowa Attorney General's Office; the Justice Research and Statistics Association; the Los Angeles (Calif.) Police Department; the National Association of Crime Victim Compensation Boards; the National Center for State Courts; the National Conference of State Legislatures; the National District Attorneys Association; the National Governors' Association; the National Organization for Victim Assistance; the National Resource Center for Domestic Violence; the National Victim Center; the New Jersey Attorney General's Office; the U. S. Department of Justice, Bureau of Justice Assistance; the U. S. Department of Justice, Office for Victims of Crime; the U. S. Department of Justice, Violence Against Women Office; the U. S. Department of the Treasury, Internal Revenue Service; and the U. S. Department of the Treasury, U. S. Secret Service. The project staff also benefitted from the advice and counsel of a consultant from the Pennsylvania Coalition Against Domestic Violence.
The resource group met once, in April 1995. The project staff presented an overview of relevant state statutory provisions at the meeting. Meeting participants provided briefings on their need for access to address information and current practices used to secure the confidentiality of such information. The participants explained the implementation of their policies, their ability to enforce them, and suggested methods for increasing confidentiality. The briefings provided the foundation for the resource group's discussion of the feasibility of maintaining the confidentiality of addresses.

The resource group identified and discussed a number of issues, including achieving a balance between the conflicting goals of increasing and facilitating public access to address information for legitimate purposes and initiating measures to protect domestic violence victims from contact with and abuse by their batterers; managing oftentimes burdensome administrative and operational requirements associated with securing the confidentiality of such information; and assessing the efficacy and feasibility of holding information sources liable for improper dissemination of information.

The recommendations contained in this report were developed from the resource group's discussion. No formal votes were taken. Rather, the recommendations presented in this report reflect the consensus of the resource group members. If the group was unable to reach a consensus, the various options that were discussed are presented.

**Principles that Guided Development of the Report**

In developing the recommendations contained in the report, resource group members and the project staff were guided by several key principles and considerations that helped to provide a context for the recommendations.

An overriding concern was to develop recommendations that would protect individuals' privacy while still allowing authorized entities to access information for legitimate purposes. The resource group recognized that access to personal information is necessary for certain legitimate purposes, and that it
therefore would be impracticable to bar completely dissemination of personal information. Likewise, the group acknowledged that the policies and procedures for safeguarding information would vary between the public and private sectors. For example, information held by public agencies may be safeguarded through statutory requirements, whereas the private sector relies on self-regulation. In addition, public agencies may require the information to carry out their functions, whereas private companies use the information primarily for commercial purposes. This distinction may affect the types of policies that are implemented.

It was the consensus of the resource group that the project should attempt to identify as many potential sources as possible through which batterers might secure their victims' addresses. However, the group recognized that it would be impossible to identify all incidental situations in which an individual might be able to obtain address information. Therefore, the group focused on areas that provide individuals with the easiest access.

At the outset, the resource group recognized that domestic violence is a very serious problem. Because of time constraints imposed by the project, however, the resource group refrained from discussing substantive issues related to domestic violence. The group decided to focus on the issue raised in the congressional mandate directing that the project be undertaken: how to protect a victim who has attempted to keep her location private from discovery by a batterer or stalker.

Definitions and Scope of the Report

The language of the congressional mandate limits the constituency of domestic violence victims to be covered by the project to spouses and ex-spouses. The resource group nevertheless decided to include recommendations that would be applicable to a broader range of relationships, including dating relationships or familial relationships, because similar concerns regarding abusers' access to information arise in this broader context.
Further, the congressional mandate did not define the word “abuse.” However, the resource group agreed that the word “abuse” would be interpreted to mean both mental and physical abuse.

The congressional mandate specifies that the report should include a study of both “addresses” and “locations.” Therefore, the resource group agreed that the recommendations would encompass both the availability of residence addresses or legal domiciles as well as other locations where a victim could be found, for example, schools, places of employment, shelters, or other organizations that a victim may visit regularly. The report uses the word “address” generally to refer to all of the above locations.
CHAPTER II
CURRENT PRACTICES IN THE PUBLIC SECTOR

Introduction

In compiling the report, the project staff examined federal statutes, such as the Privacy Act, that govern the disclosure of personal information contained in federal records; U. S. Postal Service (USPS) address correction and mail-forwarding regulations, which may provide mailers with access to individuals’ addresses; U. S. Department of the Treasury, Internal Revenue Service (IRS) regulations and policies on confidentiality; state statutes regulating the disclosure of address information from motor vehicle records, voter registration records, and other publicly held records; local school district policies; and state and federal case law addressing implementation of statutory requirements.

In addition, the project staff summarized the resource group’s discussion and recommendations on implementation of policies and statutes, and ways to prevent violations.

Federal Statutes and Policies

Several federal statutes and regulations promulgated by federal agencies govern the disclosure of information about individuals. The project staff examined the Freedom of Information Act (FOIA), the Privacy Act, the Driver Privacy Protection Act (DPPA), the Family Violence Prevention and Services Act (FVPSA), the Victims of Crime Act (VOCA), the Family Educational Rights and Privacy Act (FERPA), regulations of the USPS, and regulations of the IRS.
The FOIA, enacted in 1966, generally requires disclosure of records maintained by federal agencies, including, among other things, agency decisions, policy statements, and rules of procedure. However, the FOIA establishes many exceptions to this requirement. For example, an agency need not disclose records that might affect national security, are considered trade secrets, or are personnel or medical files that would constitute an invasion of privacy if disclosed.

In 1974, the Congress enacted another statute, the Privacy Act, which exempts additional information from FOIA disclosure. The Privacy Act specifically prohibits the disclosure of information about an individual contained in any agency record unless the individual to whom the information pertains provides written consent, or the disclosure is pursuant to an exception. The individual’s consent is unnecessary if the disclosure is to the following individuals or agencies: an employee of the agency who maintains the information, if the information is necessary to the performance of the employee’s duties; the public, if the information is part of a final opinion or policy statement of the agency, or if the information is disclosed in accordance with published rules permitting disclosure; the U. S. Department of Commerce’s Bureau of the Census; an individual who is compiling statistical information, provided that the information does not identify specific individuals; the National Archives, for historical purposes; law enforcement officials or agencies; an individual who has shown that the information is needed because of compelling circumstances affecting the health and safety of that individual or another person, as long as notification of the disclosure is sent to that individual’s last known address; the Congress; the Comptroller General; an individual who has obtained a court order; or a consumer reporting agency.

The Privacy Act also requires that the agency maintain a record of the date, nature, and purpose of each disclosure, and the name and address of the person to whom disclosure is made. This record must be made available to the individual in the record upon request.

Under the Privacy Act, an agency may not sell or rent an individual’s name and address unless such action is specifically authorized by law. Names and addresses that are otherwise permitted to be released by law are not subject to this provision.

Driver Privacy Protection Act

The DPPA, enacted in 1994, generally prohibits state motor vehicle departments’ disclosure of personal information of licensed drivers. States must comply with its provisions by September 1997. Under the law, only individual requesters may obtain information if they seek information about their own record, or have the written permission of the subject of the information. The DPPA also authorizes states to contact the subject of the information to obtain consent before disclosure.

Certain individuals and agencies still may obtain access to personal information without authorization from the individual: government agencies; courts; individuals who seek the information for use in connection with matters related to motor vehicle theft or safety; businesses and insurance companies for use in verifying their records or correcting their records to prevent fraud, pursue a lawsuit, investigate a claim, or collect a debt; researchers for statistical purposes, as long as the individual is not identified; private investigators, for an authorized purpose; employers who wish to determine the accuracy of commercial driver information; and bulk mailers, as long as individuals are provided the opportunity to prohibit disclosure of personal information. A violation of the statute may result in civil or criminal penalties.

---


Family Violence Prevention and Services Act and Victims of Crime Act

The federal government requires domestic violence shelters that receive federal funds to have confidentiality provisions. Under both the FVPSA and the VOCA, the address of a shelter may not be released without the authorization of the directors or operators of the shelter.10

Family Educational Rights and Privacy Act

Under the FERPA, an educational institution or agency is precluded from obtaining federal funds if it permits the release of "personally identifiable information" about a student unless the institution or agency has either obtained the written consent of a parent or an adult student, or the institution has classified the information as "directory information."11 If the institution has classified the information as directory information, it must notify publicly parents or adult students that the directory information will be released to the public unless the parent or student requests that the information remain confidential. The school must allow the parents or students a reasonable time to respond to the notice. Under the statute, directory information includes:

- the student's name, address, telephone listing, date and place of birth, major field of study, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance, degrees and awards received, and the most recent previous educational agency or institution attended by the student.12

According to the regulations promulgated to implement the FERPA, a school may narrow further the categories of information it classifies as directory information.13 Thus, the type of information a school characterizes as directory information may determine whether the information is subject to disclosure.

---


12 Id.

The FERPA allows the following individuals and agencies to continue to obtain records without written consent: parents of a dependent student; education officials; individuals who have obtained a court order; law enforcement officials; other schools in which the student seeks to enroll; financial aid agencies; agencies seeking to improve the quality of education if the student will not be personally identified; accrediting organizations; and in emergency situations, individuals who must have the information to protect the health or safety of the student or other persons.

Postal Regulations

Until recently, the Postal Service, for a $3 fee, would provide individuals with the new address of an individual who had filed a change of address request. In December 1994, stating that “the Congress has not given the Postal Service the function of serving as a national registration point for the physical whereabouts of individuals,” the USPS amended its rules to eliminate this service.14

Under the amended USPS rules, the service will continue to be available to individuals who wish to locate a business or organization that has relocated. Information from individuals’ and families’ address change forms will be made available only to the following individuals or entities, on proper written application: federal, state, or local government agencies for official purposes; legal process servers, attorneys, or persons representing themselves in legal actions; and individuals who have obtained a court order that requires access to the information. Law enforcement agencies will be able to obtain the information by oral request.

If an individual files a copy of a protective order with the USPS, only government agents, law enforcement officials, and individuals with court orders will be permitted to obtain the individuals’ new address. Thus, legal process servers, attorneys, and individuals representing themselves in legal actions

---

need a court order to obtain the address of a person who has filed a copy of a protective order with the USPS.

The USPS offers a variety of address correction and forwarding services, some of which may provide mailers with access to individuals' addresses. For example, if a person files a forwarding order with the post office, his mail is forwarded to his new address for one year. After that, the postal service returns the piece of mail to the sender with the new address noted on the mail piece and a note that the forwarding order has expired. The sender must re-send the letter to the new address with additional postage. This service is provided for six months after a forwarding order expires.

A sender also may request an "address correction." The sender receives notification of the new address for a .50-cent fee. A representative from the postal service told the project staff that while this service is generally available, it primarily is used by bulk mailers.

A USPS spokesperson told an NCJA staff member that once the USPS has an address in its system, it is difficult to ensure its confidentiality. Therefore, the USPS recommends that domestic violence and stalking victims not provide the post office with a forwarding order. If a forwarding order is not provided, mail that is sent to the old address will be returned to the sender with a notice on the mail piece that states "moved, left no address." Domestic violence and stalking victims who wish to have their mail forwarded, may request a temporary forwarding order. This service allows mail to be forwarded for 12 months. Subsequently, instead of returning the mail piece to the sender with the new address noted and an explanation that the forwarding order has expired, mail is returned to the sender with a "moved, left no address" notice.


16 A provision of the postal service regulations states, "If the location of a residence or place of business is known to a Postal Service employee, whether as a result of his official duties or otherwise, the employee may, but need not, disclose the location or give directions to it. No fee is charged for such information." 39 C.F.R. 265.6(d)(7).
Internal Revenue Service Policies

Because the congressional mandate required that recommendations be made regarding the methods of keeping address information confidential, the NCJA staff invited the IRS to provide a description of its policies to the resource group. The IRS, which operates under strict confidentiality statutory provisions, has earned a reputation for keeping information confidential, as well as for preventing and punishing violations of its confidentiality policy.

Statutory Authority

Section 6103 of the Internal Revenue Code deals with the confidentiality of tax returns and return information -- information that is gathered for tax administration purposes, even if it is not included on a tax return. The statute has been in effect for almost 20 years and details the circumstances under which disclosure is permitted. All information is confidential and cannot be disclosed to anyone, including IRS employees, unless disclosure is provided for in the statute. The IRS has been opposed to expanding disclosures under this section for non-tax administration purposes.

Ensuring Compliance

The IRS has disclosure officers who are experts on the Privacy Act, the FOIA, and the IRS confidentiality provisions involved in educating new employees. They also conduct awareness sessions on confidentiality during continuing professional education classes and staff meetings. They assist supervisors in reviewing the code of conduct with employees as it pertains to protecting confidential information.

The IRS commissioner has issued a delegation order that states which employees are authorized to release confidential information. The disclosure officer, in certain cases, decides whether information can

be disclosed. Disclosure officers also are the principal advisers to other officials who must decide if information should be disclosed.

The IRS compartmentalizes information. Employees are only given access to certain information that is necessary for them to do their jobs.

The IRS conducts reviews and internal audits to determine the effectiveness of its confidentiality programs. Employees can call the IRS chief inspector’s hotline if they suspect a violation. They may call the U. S. Department of the Treasury’s inspector general if they suspect a senior official has been involved in a violation. All reports can be made anonymously.

**Relationship to Other Agencies**

Under law, the IRS is permitted to provide various items of information from individual tax returns to state tax, law enforcement, welfare, and child support agencies. Before information is released, the IRS requires the recipient agency to describe how it will protect the information. The IRS requires education, inspections, testing, computer security, and checks and balances at the agencies and the agencies’ contractors receiving the information. The recipient agencies also must provide the IRS with annual reports about education, inspections, computer security, physical security, disclosure, and any changes to their programs. The IRS conducts on-site reviews of recipient agencies.

**Sanctions**

Violations of confidentiality carry both criminal and civil sanctions. The criminal sanction for a violation is $5,000 and/or five years in prison. The civil sanction is $1,000 for each unauthorized disclosure. If the violator is a federal employee, a civil sanction is assessed against the United States.
State and Local Confidentiality Policies and Statutes

The project staff examined four types of state statutes allowing individuals to obtain personal information: statutes relating to access to public records in general, statutes allowing access to records maintained by a state department of motor vehicles, statutes authorizing access to state voter registration records, and statutes allowing crime victims to place additional restrictions on the dissemination of personal information. The statutory information presented below provides selected examples of state provisions, and it is not an exhaustive treatment of the statutes in every state. In addition, a representative from the Fairfax County (Va.) public schools provided an overview of a public school district’s policies on maintaining the confidentiality of student records.

General Public Records

Every state allows access to certain records kept by public agencies. The philosophy in support of allowing the public to inspect government records is that the citizenry must be able to monitor the actions of the government to preserve democracy. Generally, case law has established a presumption in favor of permitting access. Many courts balance the public interest in favor of disclosure against an individual’s privacy interest in determining whether disclosure of certain records should be permitted.

Some states allow public inspection of all records kept by public agencies. Massachusetts provides copies of public records for a fee. Many statutes make public records accessible unless otherwise declared confidential by state law, federal law, or court order. Many states deny public access

---


to certain categories of records. Generally, such records are those that would constitute an invasion of personal privacy if they were available to the public without limitation.\(^1\) Many states cite personnel records, medical records, criminal records, and public assistance records as records whose disclosure would constitute an invasion of privacy.\(^2\) In New York, the public does not have access to records that are confidential under state or federal law, that would result in an invasion of privacy if disclosed, or that would endanger the life or safety or any person if disclosed. New York considers the sale of names and addresses for commercial purposes an invasion of privacy unless the person consents.\(^3\) Other states determine whether disclosure would violate an individual's right to privacy under the elements of the common law tort of invasion of privacy.

In Idaho, the sale by public agencies of mailing or telephone lists without the permission of the individuals on the lists is prohibited, but the requester may compile a list himself from what would otherwise be public records; however, the sale of lists of people with professional licenses is permitted.\(^4\) In North Carolina, a public agency may not disclose government records that contain information about a private person.\(^5\) In Maryland, records that include names, addresses, and identifying numbers may not be disclosed, and an individual who unlawfully releases such information is liable for damages to the person


\(^{3}\) N.Y. PUB. OFF. LAW §87 (McKinney 1988 & Supp. 1995); §89 (McKinney 1988).


affected. Washington prohibits the disclosure of the residential addresses and telephone numbers of employees or volunteers of public agencies, and customers of public utilities.

Motor Vehicle Records

Most states specify the manner in which the disclosure of motor vehicle records should be treated. Most state provisions fall into one of four categories: those that freely allow public inspection at no cost or for a small fee; those that maintain strict confidentiality except under authorized circumstances; those that allow public inspection unless the driver requests that his address remain confidential; and those that protect certain sections of motor vehicle records.

In states that permit public inspection and copying of motor vehicle records at no cost or for a fee, the type of information a requester must provide to obtain the information varies. For example, in some states, the requester must identify himself and/or state the reason for his request before obtaining a record. In other states, motor vehicle records are considered public records, and the requester need not provide any information, or the information that must be provided is not regulated by state statute, but left either to the discretion of the custodian or to the agency’s regulatory body.


Some state statutes provide that motor vehicle records are public unless declared confidential by federal, state, or other law.\textsuperscript{30} New Mexico has a statute of this sort, but permits any person to purchase a copy of a driver's record.\textsuperscript{31} Other states do not permit disclosure for commercial purposes.\textsuperscript{32}

Several state statutes declare that motor vehicle records are confidential, and may not be disclosed except to the person who is the subject of the record, a person authorized by the subject to obtain the information, law enforcement officials, government agents, employers, and insurance companies.\textsuperscript{33}

In Kansas, the names of registered car owners are public records. However, selling, giving, or receiving lists containing addresses derived from motor vehicle records are prohibited unless the lists are being distributed to government agents, car manufacturers, or insurance companies.\textsuperscript{34} In Montana, information from motor vehicle records is available upon request, but residence addresses may not be released by the department.\textsuperscript{35} In Virginia, personal information from a driver's record may not be released. However, the definition of "personal information" does not specifically include residence addresses.\textsuperscript{36} Virginia also permits licensees to have a number other than their Social Security number listed on their driver's licenses, permitting additional protection of individuals' privacy rights.\textsuperscript{37}

"Opt-out" provisions in some state statutes permit public access to motor vehicle records unless the subjects of the records have requested that their addresses or other personal information remain

\begin{footnotes}
\item[35] \textsc{Mont. Code Ann. §61-11-105 (1993)}.
\item[37] \textsc{Va. Code Ann. §46.2-342 (Michie 1994 & Supp. 1995); 1994 Va S.B. 775}.
\end{footnotes}
confidential. For example, in Delaware, information from motor vehicle records is available upon request, but individuals may request that information about them be deleted from lists that are compiled for sale. In Louisiana, motorists involved in an accident can opt-out of commercial solicitations connected with the event. An applicant for a driver’s license in Minnesota can have his residence address classified as private upon signing a statement saying that the classification is necessary for the safety of the applicant or a member of his family.

**Voter Registration Records**

There generally are four types of voter registration statutes: statutes that allow public inspection of voter registration records; statutes that allow inspection and dissemination only for political purposes; statutes that keep the addresses of voters confidential; and statutes that allow a voter to prevent his name from being disseminated.

Among states that allow public inspection of voter registration records, several prohibit the use of such records for commercial purposes. Others place no restrictions on public inspection. In Arizona, the sale of voter registration lists is prohibited except for authorized purposes. On the other hand, it is

---


permissible to sell or distribute voter lists in Idaho and North Carolina. In Iowa, voter registration lists are available upon request, but the registrar keeps a log of who has obtained a list, and misuse of the list is a misdemeanor.

Several states prohibit the release of information about a voter except for political purposes. In Alabama, voter registration lists are not public records, and information in them cannot be released except to political parties. The sale of voter registration lists is prohibited in Hawaii, and no one may have access to them except for election or government purposes. In Oregon, the residence address of an elector is exempt from disclosure unless the public interest requires disclosure in a particular instance.

Some states have opt-out provisions. In Nebraska, voter registration records are available for public inspections but cannot be copied. The sale of lists is permitted for political purposes only. A voter can have his name removed from the public record if he files an affidavit swearing that there is a court order which states that the voter or a member of his household is facing life-threatening circumstances. If a voter qualifies under this exception, he can vote by absentee ballot. In New Mexico, voters can prohibit their names, addresses, and telephone numbers from being disseminated. In addition, a person seeking information about an individual who has not opted-out must sign an affidavit stating that he will not use the list for an unlawful purpose.

---


Legislation to Protect the Privacy of Crime Victims

Several states have enacted laws to protect the privacy of victims of crimes, particularly domestic violence, harassment, and stalking. In California, domestic violence and stalking victims may have their driver’s license and registration information removed from the public record.53 Any public record in Colorado can be made confidential if a person submits an affidavit stating that he has reason to believe that he or a family member will be subject to harassment or bodily injury if the information is disclosed.54

Information about clients in domestic violence shelters in Florida cannot be released without the written consent of the client, except to medical personnel or firefighters in an emergency, law enforcement officials who have obtained a search warrant, or other individuals who have obtained a court order requiring release of the information.55 In Tennessee, no one can be compelled to reveal the address or location of a domestic violence shelter. In addition, service of process to people living at a shelter must be done through the sheriff’s office.56

In Wisconsin, a domestic violence victim’s location may not appear on documents or records to which a defendant has access.57 New Jersey has a similar law. New Jersey enacted legislation in 1994 that also allows a domestic violence victim who has obtained a permanent restraining order to register to vote without disclosing his street address. Anyone who discloses information about a domestic violence victim from voter registration lists is guilty of a crime.58 Domestic violence victims in Washington may have their

56 TENN. CODE ANN. §71-6-208 (Supp. 1994).
names removed from voter registration records. The secretary of state cannot make addresses of domestic violence victims available except to law enforcement officials or to individuals with court orders.  

School District Policies

Fairfax County’s school records confidentiality policy is partially a result of federal and state statutory requirements and partially the result of decisions made by the school board. The county denies public access to student records. Parents may obtain information about their own children unless a court order prohibits such access. The court order must state specifically that a particular parent may not have access to the child or to his records. The school board operates under the policy that noncustodial parents have rights unless such rights have been terminated; however, the school district may take as much time as necessary to determine whether the person actually is a natural parent before it is required to disseminate information in response to a noncustodial parental inquiry. The enrolling parent is notified when an inquiry about his child is made. The enrolling parent is given preference regarding any action taken involving a child.

If a woman enters a battered women’s shelter, a child may be placed in the school that serves the geographic area in which the shelter is located. The new school reports all information regarding the child to a central office. The records are processed through the original school so that most people will not be aware that the child has changed schools. If the abusive parent goes to the old school and requests his child’s file, the file will not reflect the name or address of the new school or of the shelter. However, this


60 Some state laws apply to private schools, but other policies are determined exclusively by the school. If a child is home schooled, his home address becomes publicly available as a school address.

61 Similar access to information issues may arise regarding medical records because both parents have a right to access their children’s medical records.
procedure is only a temporary measure and the custodial parent must get a court order to prevent permanently an abusive parent from obtaining file information.

Directory information about a student in Fairfax County is limited to the student's name, activities, dates of attendance, picture, height, and weight. No addresses are made available. If a commercial concern, such as a photographer, wants to contact parents, the school will address the envelopes and mail the packets. Parent/teacher associations need access to address information for a variety of reasons, but parents are given the opportunity to prevent their address from being released for this purpose.

Selected Case Law Addressing Confidentiality of Address Information

Although the project staff did not have the resources to conduct an exhaustive analysis of pertinent case law, the staff did review a number of cases that came to its attention. These cases are representative of the legal issues that have arisen in this area. Issues covered in cases reviewed included whether a domestic violence victim must be required to disclose a residential address in order to register to vote; special circumstances under which address information generally available to the public can be exempted from disclosure; and the scope of exceptions to right-to-know laws.

Voter Registration

In 1992, the Superior Court of New Jersey held in D.C. v. Super. of Elections that a victim of domestic violence should be permitted to register to vote without disclosing her residential address.62

Generally, voter registration records in the state, which include address information, must be publicly available. In 1991, the plaintiff, identified as D.C., moved to her current address after her ex-husband repeatedly violated a permanent restraining order. D.C. was fearful that her ex-husband would attempt to locate her, and wanted to keep her place of residence confidential. When D.C. attempted to

register to vote, the defendants, the Superintendent of Elections and the Commissioner of Registration in Monmouth County (N.J.), informed D.C. that her address would be publicly available under the registration statute. She did not register to vote at that time.

In 1992, D.C. again attempted to register to vote using only a post office box number as an address. The elections officials told her that the registration application was deficient because the application required her to provide her residential address.

D.C. filed suit, alleging that she had a right to vote under the New Jersey Constitution. She also relied upon the state's 1991 Prevention of Domestic Violence Act, which requires courts to keep domestic violence victims' addresses confidential. Although the act did not specifically provide for confidentiality of domestic violence victims' addresses in other contexts, D.C. argued that its broad purpose required that she be permitted to vote while keeping her residential address confidential. The court held that because previous decisions expressed a commitment to the enfranchisement of voters, the fact that a domestic violence victim wished to keep her address outside of the public record should not prevent her from exercising her right to vote.

In reaching its decision, the court relied upon a previous decision interpreting a statute requiring an individual to live in the county for 30 days before an election. The court held that individuals who moved from one county to another within 30 days of an election should be permitted to vote in the county from which they moved to avoid disenfranchisement. The court also relied upon a state attorney general's opinion that homeless people should not be prevented from voting merely because they did not have a residence address. The attorney general ruled that although the statutory requirement of providing an address generally should be upheld, it should be waived if the requirement "would erect unreasonable barriers to voting."

Since this case was decided, the state has enacted a law specifically granting the right of a domestic violence victim to register to vote without a residential address being included in the public record.
Access for Commercial or Fund-Raising Purposes

The Supreme Court of New Jersey held in Techniscan v. Passaic Valley Water Comm'n, that if information is available to the public, the purpose for which the information will be used should not be considered in determining whether the information should be released.

Techniscan Corporation, which searched public records for profit, sought access to information about customer accounts kept by a public utility. The supreme court, in affirming the lower court’s decision that Techniscan was entitled to the information, held that there was "no reason to treat such commercially motivated ‘citizens’ seeking access differently from citizens seeking information for a purely ‘private’ reason or need."67

Once a determination has been made that records are public, the motivation for seeking access is irrelevant, the court ruled. The "right-to-know law," which defined certain public records, modified the common law right of access. Under the common law, the requester’s interest in disclosure is balanced against an individual’s interest in keeping the information out of the public realm. If records are not described as public under the right-to-know law in the state, then the common law balancing test must be used, according to the court. In this instance, the records sought by the company are public under either the common law or the right-to-know statute. Therefore, the company had a right to the information. The court wrote, “any citizen, without any showing of personal or particular interest, has an unqualified right to inspect public documents” (emphasis in the original).68

A New York court held, however that a nonprofit group could not obtain the names and addresses of persons holding rifle and shotgun permits for the purpose of soliciting membership in its organization.

67 Id. at 1250.
68 Id. at 1250-51.
Under the state’s Public Officers Law, requests for name and address information may be denied as an unwarranted invasion of personal privacy if the information is sought for a commercial or fund-raising purpose, the New York Court of Appeals ruled in Federation of N. Y. State Rifle and Pistol Clubs, Inc. v. N. Y. C. Police Department. 69

The plaintiffs, a nonprofit gun organization, filed suit against the New York City Police Department when the department refused to provide the organization with names and addresses of individuals who owned rifles and shotguns. The organization claimed that its efforts to seek new members did not constitute fund-raising because attempting to increase its membership was distinguishable from directly soliciting contributions. The court disagreed, finding that the police department had acted within its powers in denying the request because “[t]here can be little question that the direct-mail membership solicitation proposed here would constitute ‘fund-raising’ if that term is given its natural and most obvious meaning.”70 Thus, under the statute, it would have been an unwarranted invasion of privacy to release the names and addresses for such a purpose.

**Student Information**

Courts in New York and New Hampshire have held that student addresses are exempt from disclosure under their states’ public records laws. In contrast, a court in Missouri held that the names, addresses, and telephone numbers of students in a school district are not protected from disclosure under its law.

In Krauss v. Nassau Community College, a New York court held that a community college properly refused to disclose the names and addresses of its students to a private citizen.71

---


70 Id. at 281.

According to the court, the FERPA prohibited the dissemination of federal funds to any educational institution that permits the release of personally identifiable information of a student to a third person without the consent of the student or his parent or guardian. Certain individuals can still obtain information, such as law enforcement officials and those who seek it in connection with an application for financial aid. In addition, the FERPA permits institutions to release information it has classified as "directory information."

The court found that Krauss had not provided any information to show that he fit into one of the established exceptions to the FERPA. In addition, the college had chosen not to designate students' names and addresses as "directory information," and therefore was not required to release the information under this exception, according to the court.

If the record does not fall under one of the enumerated FERPA exceptions, and does not constitute directory information, a court has the discretion to order disclosure. However, the court in this case held that Krauss would have to prove a need for the information that outweighed the students' privacy interests before the court would order disclosure. Because Krauss did not prove a need, he was not entitled to a court order requiring disclosure of the information.

In determining whether disclosure was required under New York law, the court noted that the state statutes pertaining to public records prohibit the dissemination of information that would constitute an unwarranted invasion of personal privacy. Under the statute, if a requester intends to use the information for a commercial purpose, any release of the record would constitute an unwarranted invasion of privacy. The court held that because Krauss had not shown that he did not intend to use the information for a commercial purpose, the college also was justified under state law in refusing to provide Krauss with the student list.
The Supreme Court of New Hampshire held in *Brent v. Paquette* that students’ names and addresses, and the names of their parents, were exempt from disclosure under the state’s right-to-know law, which generally permits public inspection of records kept by government agencies.\(^2\)

Walter Brent, a private citizen, requested a list of the names and addresses of students and their parents in the Alton School District. Such information could be found only in the registration cards and attendance records of the school. The court upheld the school district superintendent’s refusal to release the information, in part because the names and addresses had never been compiled into a single list, and therefore there was no “public record” containing the information Brent sought.

The court further held that even if the information Brent sought was part of the public record, federal and state law prevented the superintendent from releasing it. The New Hampshire right-to-know law exempts from disclosure “personal school records of pupils.” Information on registration and attendance cards qualified as personal school records, according to the court. The state law also prohibits the release of information that would constitute an invasion of privacy. The court balanced the benefits of disclosure against the benefits of nondisclosure to determine whether public inspection would constitute an invasion of privacy, and held that such inspection would invade students’ privacy. The court relied upon the trial court’s determination that “disclosing this personal information would benefit neither society nor the children and their families, but would put the children at the mercy of pedophiles and other criminals who could do them harm.”\(^3\)

According to the court, disclosure also would violate the FERPA, because the school district received federal funds, and had not adopted a policy regarding directory information. The district had a “special education plan” that allowed names and addresses to be classified as directory information, but the school district had not publicly notified parents and students of the plan, and therefore had not provided


\(^3\) Id. at 984.
them with the opportunity to have their names and addresses removed from the list as required by the FERPA. Thus, the school district would risk losing federal funds if it released information without parental consent and without the opportunity to allow parents to delete their addresses from the list.

The Missouri Court of Appeals ruled in Oregon County R-IV School Dist. v. LeMon that students' names, addresses, and telephone numbers could be released under the state's public records law.\(^4\)

Bob LeMon, representing the Missouri National Educational Association, sought a list of students' names, addresses, and telephone numbers from the Oregon County R-IV School District. The district sought a determination from the court as to whether it was required to honor LeMon's request. The trial court ordered the disclosure of the information, and the district appealed.

The district contended that because the names, addresses, and telephone numbers of its students were found on student health information cards, they could not be released under the right-to-know law. The law requires governmental records to be open unless disclosure is barred by statute, but permits records pertaining to physical health to remain closed. The court rejected this argument, holding that LeMon did not seek health information on any student, but only names and addresses, which are not afforded protection under the state law.

The district also argued that disclosure would violate the FERPA. The court rejected this argument, finding that the school district had published notice of its intent to publish directory information, and had included in its classification of directory information the names, addresses, and telephone numbers of students. According to the court, because the school district had complied with the FERPA, which permits disclosure of the directory information, the state law that required such disclosure came into effect.

\(^4\) 739 S.W.2d 553 (Mo. App. 1987).
Rights of the Media

In 1993, a court in Pennsylvania held in the case of *Times Publishing Co. v. Michel* that home addresses, telephone numbers, and Social Security numbers were within the personal security exception to the definition of “public records” in the Pennsylvania right-to-know law, and therefore the information was protected from public disclosure. 75

William McKinney, a reporter, was refused the right to inspect and copy applications for firearms licenses that had been issued by Robert Michel, the sheriff of Erie County (Pa.). The lower court held that certain information, including addresses, telephone numbers, and Social Security numbers, could not be disclosed, but that other information, including the licensee’s name, race, reason for obtaining the license, names of personal references, and answers to background questions, could be released. In addition, the court held that for all applications that had been filed before the trial court’s ruling, only the names of the applicants could be disclosed. McKinney appealed, contending that he had a right to inspect and copy all of the information on the license applications.

For a document to be subject to disclosure under Pennsylvania’s right-to-know law, a two-part test must be met. First, the document must fall within the definition of a public record. The parties agreed that license applications were a crucial element in Michel’s decision to issue licenses; therefore, the court ruled that the were public records.

The second part of the test is to determine whether the public record falls into one of the exceptions to public availability enumerated in the statute. One of the exceptions is that the disclosure of the public record “would operate to the prejudice or impairment of a person’s reputation or personal security.” Michel maintained that disclosure of the license applications fell under this exception.

The court found that this exception would apply if the person would be subject to “harm, danger, fear or anxiety” if the information was disclosed.

---

The court addressed the three categories of information separately. In considering whether to require the disclosure of addresses, the court agreed with the lower court in finding that the disclosure of firearms licensees' addresses might subject them to burglary by individuals who could not otherwise obtain firearms legally. In addition, the addresses of abuse victims, judges, prosecutors, and law enforcement officers would be made public if disclosure was permitted, which would pose a threat to their personal security.

With respect to the release of telephone numbers, the court held that an invasion of personal privacy encompasses a threat to personal security. According to the court, because citizens of Pennsylvania have a constitutional right to privacy, and the disclosure of their telephone numbers would invade that right, the numbers should be kept confidential under the personal security exception to the public records law.

The court held further that based upon its ruling regarding telephone numbers, the disclosure of Social Security numbers also should fall under the personal security exception. The court noted that "the use of computers and Social Security numbers for indexing information allows for the retrieval of extensive amounts of personal data," and the availability of such personal data was an implicit threat to privacy. The court referred to a U. S. Court of Appeals for the Fourth Circuit decision, Greidinger v. Davis, which held that a Virginia law that required voters to disclose their Social Security numbers imposed an "intolerable burden" on the right to vote.

76 Id. at 1238.

77 988 F.2d 1344 (4th Cir. 1993).
Resource Group Discussion and Recommendations

Rights of Crime Victims

A fundamental tenet of the victims' rights movement has been that constitutional amendments are needed to guarantee these rights, among them the right to confidentiality. The resource group agreed that the victim's right to privacy is very important, but due process concerns require that access to the victim and some information about the victim cannot be denied completely to a defendant.78

Resource group members recommended that court clerks be advised always to ask a victim whether he wants his personal information to be kept confidential, and whether personal information should be deleted from documents to which a defendant has access. However, the resource group acknowledged that there may be constitutional problems with such an approach because a defendant may have a right to certain information about his accuser to assist him in conducting a proper defense. One resource group member noted that whenever the constitutional rights of a victim are in conflict with the rights of a defendant, the victim's rights are always compromised, and something should be done to address that issue.

One resource group member expressed concerns about placing too many burdens upon the victim. It is already difficult for a victim to learn all the steps he must take to protect himself, the member asserted.

Statutes, Regulations and Public Policies

A resource group member noted that if the aim of a statute or regulation is to protect privacy, the actual practice of the individuals who are charged with implementing the statute or regulation, rather than the actual language of the legislation, is the critical factor. He advocated moving toward a strict liability standard, in which a person who violates privacy laws or regulations would be subject to high fines.

78 The resource group did not engage in an extensive discussion regarding defendant's rights to information about their accusers. State laws vary concerning the scope of discovery or required evidence disclosure in criminal cases.
The resource group recommended that research be conducted to determine the effectiveness of programs that permit the addresses of domestic violence victims to remain confidential by requiring that such victims be contacted through the secretary of state. The state of Washington has such a program, and a resource group member noted that a bill pending in New Jersey would establish a similar program.

Resource group members expressed concern that in attempting to solve societal problems, the government has been collecting more personal data about individuals. For example, new laws aimed at enforcing court orders requiring the payment of child support have resulted in the increased collection of personal information about both individuals required to pay child support and recipients of child support. This increased collection of personal data has raised concerns about protecting the privacy interests of those in the welfare and child support systems. Another member was concerned about the use of Social Security numbers as identification in a variety of situations. In addition, one member noted that it is impossible to require national identification systems on the one hand, and still protect the privacy of domestic violence and stalking victims on the other. The more uses to which a person’s Social Security or other identifying number is put, the more an individual’s anonymity and privacy are lost, the resource group member observed.

Resource group members expressed concern that the purpose for which information is collected is not always the purpose for which it ultimately is used. Once the information exists in certain records, it is difficult to restrict how it will be used. Thus, some resource group members recommended that information be collected and disseminated only when there is an absolute need to know the information to carry out duties.

The resource group agreed that an agency should always require a requester to state the reason for which the information is needed, and should keep track of the identities of requesters.
CHAPTER III
CURRENT PRACTICES IN THE PRIVATE SECTOR

Generally, private entities are not subject to state or federal law governing the disclosure of information. However, increasing concerns about maintaining the confidentiality of personal information have prompted private companies that keep such information for business purposes to establish policies regarding confidentiality and the release of information to the public. Such self-regulation may occur in a variety of ways. Trade associations may establish industry-wide guidelines, which their members are required to follow. Individual companies also may establish their own policies and sanction employees who violate these policies.

The project staff invited representatives from the Bell Atlantic Corporation, the Direct Marketing Association (DMA), the Associated Credit Bureaus (ACB), and the Information Industry Association (IIA) to provide an overview of their policies and practices to the resource group. The project staff also examined the policies of legal data base services and the availability of information through a commercial background check service.

Bell Atlantic Corporation's Privacy Policies

Bell Atlantic recently adopted an information privacy code that explains to customers how the company uses information about them. The privacy code is being mailed to new customers and will be published in the White Pages in future telephone directories. The code and other policies are reviewed with new hires and with other employees on an annual basis. A violation of the privacy code may result in dismissal.
Use of Information

Address information must be gathered by Bell Atlantic to provide, maintain, and bill customers for services, but the company offers options to customers about how that information will be disseminated. In addition to removing names from telephone directories and directory assistance, customers can limit the amount of information that is published about them. For example, a customer can exclude address information or only have a first initial listed in the directory.

Bell Atlantic provides published lists from directories to companies for direct marketing purposes, but it reserves the right to review the information that will be sent to companies to verify that the lists are not being abused. Persons who already are not published or listed in directories are omitted from these lists; other customers are given the opportunity to opt out of lists provided for direct marketing purposes.

Some of Bell Atlantic’s services allowing customers to prevent the dissemination of their telephone numbers require the payment of a fee. Call blocking, listing options, and omitting names from marketing lists are free services, but removing a name from a directory requires the payment of a small fee. The federal government requires Bell Atlantic to compile directories, and a portion of the fees collected covers the cost of this mandate.

Security

Bell Atlantic employs about 60,000 people and uses a number of different security measures. Information is compartmentalized so that only persons who need information will have access to it. For example, installers are provided with only the information necessary to install a telephone.

Computer passwords for those who have access to personal information are changed on a monthly basis. There are electronic trails left when an employee accesses information. In addition, employees are provided a telephone number that they can call to report suspicions that a violation has occurred.
Caller ID

Bell Atlantic first began offering Caller ID because it believed that parties had a right to know who was calling them. The service allows a subscriber to see the telephone number of the person who is calling them on a monitor. To respond to concerns from domestic violence groups and others, Bell Atlantic began to offer per-call blocking, which allows a caller to block his number from appearing on a recipient’s Caller ID if the caller enters a code before dialing.

In addition, subscribers to Caller ID can choose not to accept calls from particular numbers. If a subscriber chooses to exercise this option, a call from the chosen numbers will not go through and the number will not appear on the Caller ID unit. Bell Atlantic is expecting the Federal Communications Commission to require per-call blocking anywhere that Caller ID is available.

Per-line blocking, which presently is available statewide only in Pennsylvania and on a limited basis in other areas, allows a caller to block his number from appearing on a “Caller ID” unit at all times. If a recipient has the “anonymous call rejection” service, however, a caller must unblock the call or the line to get through to the recipient.

Caller ID has a good track record in reducing the number of harassing and obscene calls, according to the Bell Atlantic representative. When it was first introduced in New Jersey, there was a 70-percent reduction in the number of complaints about harassing calls. Bell Atlantic has continued to work with domestic violence groups to offer additional protection in this area.

79 In response to a question from a resource group member, the Bell Atlantic representative clarified that Caller ID does expose the caller’s number to any individuals called from the unit.
Direct Marketing Practices

Use of Information

The DMA compiles lists of names and addresses of individuals who might be interested in particular products or services. Its information is obtained from members' customer lists. The DMA representative noted that because of concerns about competition, only about 50 percent of direct marketers provide their customer lists to other companies.

Individuals may have their names removed from direct marketing mailing lists by writing to the direct marketing company or the DMA. The DMA has conducted consumer education campaigns to inform consumers how the direct marketing industry works.

Direct marketers do not give out specific information about an individual primarily because it is prohibitively expensive to extract individual information from lists. Direct marketers use listings of the names of hundreds of thousands of people who may have an interest in a general area. The DMA representative said that it is unlikely that direct marketing lists would be used to access information on a single individual.

The DMA has opposed government agency access to its data bases. For example, the DMA successfully opposed an attempt by the IRS to gain access to the DMA's data bases for purposes of trying to identify possible tax evaders. The information in the data bases is collected for commercial reasons and should not be used for any other purpose, according to the DMA representative.

Guidelines and Policies

The DMA has developed guidelines for marketers, one of which requires them to inform consumers periodically that the data ultimately may be rented, sold, or exchanged and that they are being given the opportunity to opt out. The guidelines also address security issues.
The DMA developed a manual to provide direct marketers with guidance, and has had a privacy task force in place since 1989.\textsuperscript{80} The task force has been working on self-regulatory programs, including those concerning privacy issues. It is charged with ensuring that the DMA is building consumer trust and confidence. A DMA representative noted that it is important to remember that lists not only are used by direct marketers looking to market products, but also by nonprofit and political organizations interested in fund-raising.

Credit Bureau Policies

The ACB represents TRW and Equifax, as well as several smaller credit bureaus and collection agencies. The ACB subscribes to most of the same guidelines as the DMA. According to the ACB representative, there is a need to balance the concerns of the business community with the concerns of individuals, and the ACB would support fully anything within reason that can be done to protect victims of domestic violence. The ACB was not aware of any instance in which credit bureau information was used to gain access to a battered spouse, but if it had been used for such a purpose, the ACB would like to be informed so that it could attempt to institute measures to prevent further abuses.

The ACB requires that its members follow the requirements of the Fair Credit Reporting Act (FCRA),\textsuperscript{81} which was enacted to ensure that credit bureaus adopt reasonable procedures for meeting businesses’ legitimate needs for credit information and ensuring that these procedures are fair to consumers regarding confidentiality and accuracy. The FCRA places strict limits on who has access to credit reports.

The ACB is concerned about contradictions between the FCRA and other laws. For example, the IRS had proposed giving it access to credit reports for the purpose of finding tax evaders. After the ACB challenged the proposal on the grounds that it violated the FCRA, the IRS withdrew the proposal.


The ACB works to protect a consumer's right to privacy; however, there are legitimate circumstances when personal credit information should be made available to certain parties. Members of the ACB are required to show who has access to information and for what purpose it will be used. A member of the public may not have access unless he has a court order showing the purpose of his request. Regardless of how many security measures are in place, an individual who wishes to break the law will be able to do so, according to the ACB representative.

The ACB has an active education program through which it encourages its members to train employees. The ACT noted that a big concern is that the U. S. Department of Justice and the Federal Trade Commission do not consider certain kinds of scams or violations of the FCRA important enough to prosecute.

Information Industry Association Guidelines

The IIA, a trade association representing companies involved in the creation, distribution, and use of information products, services, and technologies, has encouraged companies to take steps to protect "personally identifiable information" and to explain their policies and practices regarding the collection, use, and distribution of information.82

The IIA recommends that companies establish a policy regarding the personally identifiable information they collect, make the policy publicly available, review and update it periodically, and establish a method for monitoring compliance.

In addition, the IIA encourages companies to take steps to ensure that personally identifiable information is protected from loss, misuse, disclosure or destruction.

The IIA suggests that when a company obtains information from an individual, the company disclose to the individual how it intends to use the information, and that the information be used only in a manner that is consistent with that intention.

Companies also are encouraged to establish a procedure in which individuals can determine whether the company has information about them, and are able to correct or delete inaccurate or incomplete information.

**Computerized Legal Data Bases**

Computerized legal data bases maintained by Lexis/Nexis and Westlaw provide personal information compiled from a variety of sources to individuals who subscribe to these services. The information compiled in the data bases generally is obtained from property records; U. S. Department of Commerce, Bureau of the Census information; telephone directories; student directories; motor vehicle records; corporate asset records; bankruptcy records; lawsuit filings; professional license records; U. S. Postal Service information; newspapers; and birth announcements.

Lexis/Nexis and Westlaw provide these services to assist investigators and attorneys in locating individuals and assets while preparing for litigation. Each company maintains a “people locator” data base and an “asset locator” data base. The “people locator” data bases include address, telephone, and other information obtained from telephone directories and other sources. The asset locator data bases include information from property records. Lexis/Nexis permits individuals to have their names removed from the people locator data base upon request, but will not delete information from the asset locator data base because it is from public records. Removal of the record may take up to 12 weeks. Westlaw will not delete information from either data base, reasoning that because the information is available in public records, it does not compromise individual privacy rights to maintain the information in the data base.
Because information from all 50 states readily is available in one place, the computerized data bases minimize the time and effort necessary to locate an individual. Thus, legal data base services may wish to examine the policies regarding the availability of such information to determine whether there are ways to ensure the services are not used for illegal purposes.

Discussion and Recommendations of the Resource Group

A member of the resource group commended Bell Atlantic for its toll-free service that permits customers to obtain information about privacy. The technological revolution requires that persons relearn telephone habits in order to maintain privacy, and the toll-free service is helpful in this way.

Children are unlikely to understand the dangers that may result from certain uses of the telephone, and may unknowingly place individuals in shelters in danger by using the shelter telephone, the resource group member continued. Consequently, children should be taught how to use the telephone, what services are available, and should be properly supervised. The resource group member also expressed appreciation for the fact that address information will not be available through Caller ID.

Many people do not realize that the person they are calling may have Caller ID and that they may be transmitting their telephone number to the person they are calling. It is difficult for the telephone company to be responsible both for marketing the service and also for providing education about its potential consequences, according to one resource group member.

Some members of the group noted that in an effort to provide increasingly fast service through better technology, private companies may be compromising privacy rights. For example, in California, a person may access his own motor vehicle records through an electronic kiosk system. Although individuals generally may not access other individuals’ information, once the information is in the system, it becomes easier to access unlawfully.
Some members of the group expressed concern over the dissemination of health care information. As large health maintenance organizations become more prevalent, more individuals are able to have access to medical records, possibly compromising their security.

In the private sector, where personal information generally is used for commercial purposes, some resource group members recommended that individuals always be allowed to decide whether their information will be available on certain lists. Recognizing that the best way to ensure that information is not disclosed is to ensure that a record is not available in the first place, one resource group member suggested that abuse victims should be able to have their names deleted from any private data source upon request. Although most private companies allow an individual to have his name removed from their lists, a resource group member noted that perhaps there should be an opportunity to "opt-in" rather than "opt-out." Domestic violence victims are more concerned about their safety than about receiving solicitations from marketers, and many are not aware of their options, according to one member. Therefore, some resource group members suggested that organizations adopt policies that would prevent information from being disseminated unless an individual has consented to its release.

One resource group member suggested that individuals or businesses seeking to obtain information from other private sources should be required to provide a statement of the purpose for which the information is being sought, and an assurance of the organization's methods for preventing the improper dissemination of information.
CHAPTER IV
RESULTS OF A SURVEY TO DETERMINE VARIOUS METHODS OF PROTECTING THE CONFIDENTIALITY OF A DOMESTIC VIOLENCE VICTIM'S LOCATION

Methodology

Because there has not been any conclusive research done regarding how addresses are obtained by batterers and stalkers, the NCJA sent informal surveys to the domestic violence coalitions in the 50 states to obtain additional information about their experiences in this area.

The survey asked six questions designed to obtain information from the coalitions about difficulties encountered in maintaining the confidentiality of domestic violence victims' locations, and recommendations for further action (see Appendix C). The survey asked the coalition representatives to gauge how difficult it is to protect disclosure of a victim's location to a batterer; to identify the principal sources of information for batterers who are trying to locate victims; whether the legislatures in their states have taken steps to prevent the dissemination of personal information; and to suggest additional steps that might be taken to prevent batterers from locating victims. In addition, the survey asked what types of precautions are taken by a domestic violence shelter to prevent disclosure of its location, and what steps are taken to protect residents of a shelter if a batterer determines its location.

The project staff received 31 responses from 22 states. Some coalition representatives sent the survey to individual shelters in their states. Therefore, in some instances, the project staff received several responses from one state.

83 Responses were received from Alabama, Colorado, Florida, Hawaii, Illinois, Louisiana, Maryland, Massachusetts, Mississippi, Nevada, New Jersey, North Carolina, Ohio, Rhode Island, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, West Virginia, and Wisconsin. See Appendix D for a list of respondents.
Summary of Results

Each survey question is reprinted in italics below. A summary of the responses to the question follows.

1) In your experience, how difficult is it to protect a domestic violence victim's address or location from a batterer?

The majority of respondents stated that it is very difficult to protect a victim’s location. Three respondents answered that it was not difficult in their state, particularly if the victim was in a shelter. Several survey participants stated that the problem was graver in rural areas, or if the victim has children who may not recognize the necessity of maintaining confidentiality.

2) What are the principal sources batterers use to secure the addresses or locations of their victims? Please provide the sources of information on this issue.

The most common sources mentioned by survey participants were family and friends; children’s school records; court documents; Caller ID; the post office; stalking the victim by appearing or following him to places he frequents; motor vehicle records; telephone records; the police department; filing kidnapping charges against a victim who takes children with him; welfare records; and the victim’s employer or coworkers.

Other sources that were mentioned included: state requirements that women seeking an abortion notify their spouse of their intent; notification requirements in paternity cases; taxi drivers; bank records; medical records of children; the public housing authority; the media; private investigators; professional, marriage, driver, or pet licenses; Social Security records; unsupervised visitation with children; voter registration records; and individuals who work at a place where the victim is likely to go, e.g., a maintenance person at a shelter.

---

84 Florida Coalition Against Domestic Violence, Hawaii State Committee on Family Violence, and Vermont Network Against Domestic Violence & Sexual Assault
The respondents generally obtained the information to respond to this question from shelter staff and victims. In some cases, police officers, victims' family members, and employees of the telephone and postal systems provided information that was used by respondents to complete the survey.

3) What, if any, steps has your state taken to prevent dissemination of personal information through public sources of information such as court records, motor vehicle records, voter registration records, etc.? If the state has taken steps to prevent dissemination of personal information, are the regulations applicable only to domestic violence victims? If not, are there additional steps a domestic violence victim may take to further protect his address or location? Please provide the citations to any statutes that prevent the dissemination of personal information through public sources.

The following information is based solely upon the responses provided by the survey participants, and has not been verified by the project staff. Citations have been listed only if the representative provided a citation with his response. For further information on statutory provisions, see Chapter II.

In Florida, legislation has been enacted to ensure confidentiality between a domestic violence advocate and a victim.85

A number of states make address information on court records confidential. In Massachusetts, for example, an individual only may petition the court to have his address expunged from court records if he has "good cause." A court generally will not grant the petition unless the victim has obtained a protective order.

In New Jersey, a domestic violence victim's address may not appear on court documents,86 shelter addresses remain confidential, and victims who have obtained restraining orders need not disclose their address to vote.87 In South Dakota and Utah, providing an address or a telephone number on a protective

order is optional. In Vermont, the family court will keep the location of parties to an action confidential. Wisconsin prohibits the disclosure of a victim’s address in petitions for harassment restraining orders.\(^8\)

The New Jersey Board of Regulatory Commissioners has issued regulations for Caller ID that allow the service to be blocked free of charge for any subscriber; per-line blocking is available for domestic violence programs and for any person with an unlisted number.

Under Tennessee’s Victims of Crime Act, no one may be coerced to disclose shelter locations.\(^9\) A law in Wisconsin prohibits battered women’s programs from disclosing the whereabouts of domestic violence victims and their children.\(^{10}\)

Illinois allows a court to issue protective orders that prevent the dissemination of school records. In addition, the secretary of state may protect the motor vehicle records of domestic violence victims. The Motor Vehicle Division and utility companies may be prevented from disclosing addresses upon request in Texas. In Utah, information from the motor vehicle registry is protected upon request, and address information is omitted from drivers’ license records. In Vermont, motor vehicle information is confidential. Access to motor vehicle records has been limited in Virginia.

One respondent from Hawaii said that motor vehicle and voter registration records are confidential. Another said that voter registration records are publicly available, and yet another survey participant said that although the records are confidential in Hawaii, public employees may give out information at their discretion, and many are overworked, so they may not take the time to determine the circumstances surrounding a request before disclosing the information.

Respondents provided three ways in which domestic violence victims can take further steps to protect their addresses or locations. First, victims should send copies of restraining orders to public

---


agencies with a letter asking that their addresses be kept confidential. Second, a victim should ask the appropriate agency for assistance in stopping the abuse. Finally, the victim should not telephone the batterer, and should prevent children from doing so.

4) What additional steps would you like state or local governments to take to prevent batterers from locating the addresses or locations of their victims?

The responses that survey participants provided for this question fell into several categories of recommendations. The first category relates to limiting the availability of information in record systems. The second involves limiting public access to information in public records. The third consists of providing the victim with more protection in the legal system. The last category relates to training individuals about the necessity of privacy protection and sanctions that should be imposed on various actors in the system if they violate an individual’s right to privacy.

Limiting Availability of Information

Some respondents suggested that certain information should not be available under any circumstances. Respondents also expressed concern that once information is collected by a state agency, it usually becomes a public record. Therefore, agencies should re-evaluate what types of information are essential for them to carry out their duties. Some respondents said that states should employ measures that would limit individuals’ ability to obtain telephone numbers through services such as Caller ID and Call Return. One respondent recommended "complete confidentiality" for all personal information.

Limiting Public Access to Information

Several respondents recommended that school and public employees, such as welfare case workers, child support enforcement officials, and law enforcement officials, should be restricted from disseminating personal information.
Additional Legal Protection for Victims

Some survey participants recommended that the court be required to balance a victim’s safety against the visitation rights of a battering spouse when determining custody and visitation issues. Others recommended that, in states that do not already provide the service, domestic violence victims’ addresses be excerpted from court documents. Some respondents recommended that discussions between a victim and a counselor be privileged, and that records kept by the counselor be protected from discovery.

In addition, some participants recommended providing free access to post office boxes and free call blocking for domestic violence victims. Finally, one respondent recommended that the state make it easier for victims to obtain a change of name and new Social Security number.

Training

Respondents recommended that school and public employees, such as welfare case workers, child support enforcement officials, and law enforcement officials be reminded continually about the necessity of protecting the identities of their clients and any personal information they may have about those clients.

One respondent recommended the implementation of a public awareness campaign on victim’s protection.

Sanctions

Survey participants recommended that the state impose sanctions on school and public employees, such as welfare case workers, child support enforcement officials, and law enforcement officials who release information about an individual without the proper authorization.

Participants also recommended increasing penalties and lengthening periods of incarceration for batterers as a way of keeping a batterer away from a victim. Others recommended the increased enforcement of restraining orders.
5) *What precautions do domestic violence programs take to protect their clients' locations from batterers?*

The categories of responses to this question include: educating victims about ways to maintain their own safety and providing the assistance of shelter staff; enforcing staff procedures to protect shelter locations and the safety of clients; and developing better record-keeping procedures.

**Victim Education and Assistance**

Respondents recommended encouraging victims to take taxis instead of public transportation when going to or leaving a shelter, encouraging victims to obtain a post office box to receive mail, and assisting clients in developing safety plans.

One respondent recommended that victims be assisted in obtaining a house alarm and/or a portable phone that is programmed to dial 911.

Survey participants mentioned several ways in which domestic violence service providers can assist clients in maintaining the confidentiality of their locations. Service providers can assist clients in petitioning courts to excerpt addresses from court documents; obtaining protective orders; changing a client's name and Social Security number; writing a letter to social service agencies to explain why information about a victim should remain confidential; and by referring them to shelters out of the area or in another state.

**Shelter Procedures**

The majority of survey participants said that shelter staff should never confirm or deny a client's presence at a shelter.

Some shelters require victims to sign confidentiality agreements before they are permitted to reside there. In addition, the shelters use post office boxes and maintain unlisted telephone numbers. Some
shelters screen clients at a separate administrative office before allowing them to know the shelter's location. Others maintain a stringent security system to prevent batterers from entering a shelter.

Some respondents said that shelter staff in their state give directions to the shelter in stages, rather than all at one time, so that if a victim records the directions on paper, a batterer who finds them will not be able to discern the route to the shelter.

**Record Keeping**

Some respondents recommended that domestic violence programs keep the records of a victim and a batterer in separate locations. In addition, unless a person has specific authorization, he should be denied access to files in a domestic violence program office.

6) *If a batterer does determine the address or location of a domestic violence shelter, what procedures do domestic violence programs in your states follow to protect residents?*

The majority of respondents said that the shelter staff immediately will call 911 and begin procedures for relocating the client to another shelter.

In addition, the shelter may obtain a protective order that prevents the batterer from coming within a certain distance of the shelter, and may bring trespassing charges against a batterer. Some shelters maintain special procedures for hiding and protecting residents.

Some respondents said that the shelter would institute a curfew. Others would ask for extra police patrols in the area.
The congressional mandate required the project staff to accomplish two objectives. The first was to provide findings regarding the sources from which abusive partners can obtain address or location information. The second was to determine what methods could be used to protect the confidentiality of such information.

In complying with these requirements, the NCJA project staff used several research methods. The first included an analysis of relevant statutory law, case law, and governmental regulations in the area of information protection. The project staff also convened a resource group and spoke with representatives from various federal and state agencies and the private sector to obtain information about the types of confidentiality policies that have been established, and the procedures in place for preventing violations. Finally, the project staff composed an informal survey that was sent to the domestic violence coalitions in each state to attempt to obtain additional information about how batterers discover the locations or addresses of abuse victims.

Information developed by the project staff through research, including the survey of state domestic violence coalitions, and consultations with resource group members, indicated that there is a broad spectrum of public and private data sources from which an abuser conceivably could secure information that would help him to locate his victim. Most of these data sources are managed by public and private agencies and organizations that have adopted strict rules and regulations to govern privacy and confidentiality.

Most public and private agencies and organizations also have put in place mechanisms to enforce these rules and regulations and a system of sanctions to be levied in cases of abuse. Contemporarily, public and private agencies are aware of the prevalence of domestic violence and the potential for these interpersonal conflicts to be brought into the workplace. These public and private agencies are
accommodating or are prepared to make accommodations for domestic violence victims in their data disclosure policies. In sum, public and private agencies generally appear to be taking appropriate steps to restrict access to information that should be kept private and confidential.

Resource group discussions pointed out that the safety of domestic violence victims may be threatened as much by the legitimate dissemination of public information as by incidents in which personal information that is not subject to disclosure is unknowingly or deliberately shared with an abuser. For example, states that permit public access to motor vehicle records have created a ready means for the abuser to use to learn the location of his victim. In such cases, public and private agencies are faced with the challenge of developing policies and managing protocols to limit or prohibit access in exceptional cases.

The resource group also asserted that notwithstanding statutes, rules, regulations, and policies, abusers nonetheless may be able to gain access to information about their victims’ locations by preying upon the sympathies and loyalties of family and friends or upon the greed or other motives of individuals who have access to this information and can be induced to share it. A decision to ignore the law or regulation no matter what the motive may have tragic consequences for the victim.

While this project determined some of the ways that abusers get address information on their victims, until more is known about the methods and data sources that abusers are using to gain access to their victim’s address or location, it will be difficult to target specific measures to control abusers’ access to this information. Nevertheless, several measures were identified that might help control abusers’ access to their victims.

- **Reviewing the adequacy of laws:** States should review privacy and confidentiality statutes to ensure their adequacy and currency.

- **Educating the public:** Public education about domestic violence should stress the need to keep confidential any information about a victim who has chosen to keep his location from the abuser.
Adopting and enforcing codes of conduct: All public and private agencies should adopt codes of conduct for employees that cover the dissemination of confidential information. All employees should receive training in the codes of conduct. These codes should include sanctions for violations and should be backed up by enforcement mechanisms. Agencies and organizations might consider instituting a hot line to encourage employees to report anonymously violations of privacy rules and regulations.

Limiting access to information: Public and private agencies and organizations should compartmentalize and limit access to sensitive information, including personnel information. Electronic trails should be built into automated data bases to monitor access to information and thereby identify potential violators.

Additional Recommendations

The resource group and other project consultants provided the following additional suggestions for maintaining the confidentiality of a domestic violence victim's location.

Recommendations to Victims and Advocates

- Domestic violence victims may wish to use the "opt-out" provision required by the FERPA to prevent the compilation of information about themselves or their children in a student directory.
- Because the USPS cannot ensure the confidentiality of an address in its system, domestic violence victims who are relocating may choose not to submit a forwarding order or to use temporary forwarding orders.
- Domestic violence victims may wish to take advantage of "opt-out" provisions provided by state statutes and businesses, which allow individuals to have personal information removed from a
variety of sources upon request. For example, in some states, subjects of motor vehicle records can request that their addresses and other personal information remain confidential.

- Domestic violence victims may wish to become educated about the variety of services available through telephone companies to ensure that their telephone numbers are not being disclosed.
- Victim advocates should be encouraged to inform victims about privacy issues and ways to keep personal information confidential. Advocates also should be encouraged to assist victims who are attempting to have their names and addresses removed from public lists.

Recommendations to States

- States may wish to consider examining their public records statutes to determine whether additional protection should be in place to protect the dissemination of personal information for unlawful purposes.
- States may wish to examine and evaluate the efficacy of programs that have been instituted to permit domestic violence victims to keep their whereabouts confidential.
- States may wish to require court clerks to ask victims whether personal information should be removed from court records to which a defendant may have access. However, due process concerns may be implicated if a defendant is denied all access to information about his accuser.
- States may wish to conduct research or quality control inspections to determine whether custodians of information are complying with statutory requirements that prevent information from being disseminated.
- States may wish to consider permitting information to be collected only if such information is needed to carry out the duties of the agency.
States may wish to consider establishing agency policies that require a requester of information to state the reason for which the information is needed, and that require agencies to keep track of the identities of such requesters.

Recommendations to Businesses

- Businesses may wish to consider always offering an "opt-out" provision to individuals to prevent information about them from being disseminated beyond the source to whom the individual provided the information in the first instance. In the alternative, businesses may wish to allow individuals to "opt-in" rather than "opt-out" of lists compiled for their services.
- Businesses may wish to consider educating their customers about how personal information about them will be used.
- As technology advances, businesses may wish to consider the implications of such technology on the privacy rights of individuals.
- Businesses may wish to consider implementing policies to assure the prevention of the improper dissemination of information.
Appendices
Appendix A:

Resource Group Meeting Agenda
Anti-Stalking/Privacy Resource Group Meetings

hosted by the

National Criminal Justice Association

April 18-19, 1995
Hall of the States
444 N. Capitol St., NW
Room 333
Washington, DC 20001

AGENDA

TUESDAY, APRIL 18

WELCOME AND OPENING REMARKS 1:00 p.m.

Gwen A. Holden, Executive Vice President
National Criminal Justice Association (NCJA)

UPDATE ON STALKING LEGISLATION AND RELATED CASE LAW

Nadine M. Rapacioli, Staff Attorney, NCJA

REVIEW OF AND COMMENTS ON REPORT FOR THE ANTI-STALKING SEMINAR SERIES

The resource group members will be asked to provide comments on the draft final report for the U. S. Department of Justice, Bureau of Justice Assistance (BJA)-funded anti-stalking seminar series.

Ms. Holden

Lisa Doyle Moran, Assistant Director for Legal Affairs, NCJA

REVIEW OF AND COMMENTS ON PAPER ON INTERVENTION IN STALKING CASES

Resource group members will be asked to provide comments on a draft paper titled “Implications of Stalkers’ Motives and Relationships with Their Victims on Intervention Strategies.”

Ms. Holden

DISCUSSION OF “BEST PRACTICES” IN STALKING CASES

Resource group members will be asked to identify programs that arguably may demonstrate the “best practices” for law enforcement, prosecutors, and victims’ advocates in managing stalking cases, which will be incorporated in a report by the U. S. Department of Justice, Office for Victims of Crime (OVC) marking the 12th anniversary of the Victims of Crime Act.

Aileen Adams, Director, OVC

Ms. Holden

RECESS 5:00 p.m.
WEDNESDAY, APRIL 19

DISCUSSION OF THE PRIVACY PROJECT'S ORIGIN, SCOPE, ORGANIZATION, AND PRINCIPAL WORK EFFORTS - 9:00 a.m.

Ms. Holden

Bernard V. Auchter, Program Manager
U. S. Department of Justice, National Institute of Justice (NIJ)

OVERVIEW OF RELEVANT STATE STATUTORY PROVISIONS

The project staff will provide an overview of state statutory provisions on the release of address information contained in motor vehicle and voter registration records.

Ms. Doyle Moran

BRIEFING ON PUBLIC AND PRIVATE NEEDS FOR ACCESS TO ADDRESS INFORMATION AND CURRENT PRACTICES USED TO SECURE THE CONFIDENTIALITY OF SUCH INFORMATION

Amy V. Anderson, Assistant Manager
Bell Atlantic Corporation, Privacy & Public Policy

Jerry Cerasale, Senior Vice President for Government Affairs
Direct Marketing Association

Albert Verville, Coordinator, Central Student Registration
Fairfax County (Va.) Public Schools

DISCUSSION OF ISSUES RELATED TO THE CONFIDENTIALITY OF VICTIMS' ADDRESSES

The project staff will facilitate a discussion of various issues concerning the confidentiality of victims' addresses. Examples of issues to be discussed include:

- the administrative burden that would fall on holders of address information if the confidentiality of such information is to be secured;
- balancing the conflicting goals of public access to address information for legitimate purposes and protection of domestic violence victims from contact and abuse by their batterers; and
- the feasibility of holding information holders liable for the improper dissemination of information.

Ms. Holden

Ms. Doyle Moran

WORKING LUNCH - 12:00 noon

DISCUSSION OF RECOMMENDATIONS TO BE MADE ON CONFIDENTIALITY OF VICTIMS' ADDRESSES

Ms. Holden

Ms. Doyle Moran

ADJOURN - 3:00 p.m.

---

91 A continental breakfast will be available beginning at 8:00 a.m.
Appendix B:

Resource Group Participant List
PARTICIPANTS

Anti-Stalking/Privacy
Resource Group Meetings

April 18-19, 1995
Washington, DC

Ms. Aileen Adams
Director
Office for Victims of Crime
U. S. Department of Justice
633 Indiana Avenue, NW
Washington, DC 20001
Tel.: (202) 307-5983
FAX: (202) 514-6383

Ms. Amy V. Anderson
Assistant Manager
Privacy & Public Policy
Bell Atlantic Corporation
1310 N. Courthouse Road
Arlington, VA 22201
Tel.: (703) 974-5999
FAX: (703) 974-0780

Mr. Bernard V. Auchter
Program Manager
Family Violence Research Program
National Institute of Justice
U. S. Department of Justice
633 Indiana Avenue, NW
Washington, DC 20531
Tel.: (202) 307-0154
FAX: (202) 307-6394

Mr. David Beatty
Director of Public Policy
National Victim Center
2111 Wilson Blvd., #300
Arlington, VA 22201
Tel.: (703) 276-2880 X147
FAX: 703) 276-2889

Ms. Diana J. Burleson
Senior Attorney
American Prosecutor Research Institute
99 Canal Center Plaza, Suite 510
Alexandria, VA 22314-1503
Tel.: (703) 549-9222
FAX: (703) 836-3195

Mr. Jerry Cerasale
Senior Vice President
for Government Affairs
Direct Marketing Association
1111 19th Street, NW
Suite 1100
Washington, DC 20035
Tel.: (202) 955-5030
FAX: (202) 955-0085

Ms. Lorna Christie
Vice President for
Consumer Affairs
Direct Marketing Association
1111 19th Street, NW
Suite 1100
Washington, DC 20035
Tel.: (202) 955-5030
FAX: (202) 955-0085

Mr. John Bender
Deputy Attorney General
Law Division
Office of the Attorney General
Richard Hughes Justice Complex
Trenton, NJ 08625
Tel.: (609) 984-1053

Ms. Lorna Christie
Vice President for
Consumer Affairs
Direct Marketing Association
1111 19th Street, NW
Suite 1100
Washington, DC 20035
Tel.: (202) 955-5030
FAX: (202) 955-0085
Appendix C:
Confidentiality of Domestic Violence Victims’ Locations Survey
Confidentiality of Domestic Violence Victims' Locations
Survey

Organization:

Address:

Person Completing Survey:

Telephone Number:

1) In your experience, how difficult is it to protect a domestic violence victim’s address or location from a batterer?

2) What are the principal sources batterers use to secure the addresses or locations of their victims?

   a) Please provide the sources of your information on this issue.
3) What, if any, steps has your state taken to prevent the dissemination of personal information through public sources of information such as court records, motor vehicle records, voter registration records, etc.?

a) If the state has taken steps to prevent dissemination of personal information, are the regulations applicable only to domestic violence victims? If not, are there additional steps a domestic violence victim may take to further protect his or her address or location?

b) Please provide the citations to any statutes that prevent the dissemination of personal information through public sources.
4) What additional steps would you like state or local governments to take to prevent batterers from locating the addresses or locations of their victims?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

5) What precautions do domestic violence programs take to protect their clients' locations from batterers?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

6) If a batterer does determine the address or location of a domestic violence shelter, what procedures do domestic violence programs in your states follow to protect residents?

________________________________________________________________________

________________________________________________________________________

________________________________________________________________________

Please return by July 15, 1995, to:

Privacy Survey
c/o NCJA
444 N. Capitol Street, NW
Suite 618
Washington, D.C. 20001
FAX: (202) 508-3859
Appendix D:

Respondents to Confidentiality of Domestic Violence Victims' Locations Survey
Alabama
Alabama Coalition Against Domestic Violence

Colorado
Boulder County Safehouse
Community Housing Services Inc.
Elder Abuse Prevention Program
Domestic Violence Initiative
Family Tree
Safehouse Denver, Inc.

Florida
Florida Coalition Against Domestic Violence

Hawaii
Hale Ho'omalu Shelter
Hawaii State Committee on Family Violence
The Family Crisis Shelter, Inc.
Women Helping Women
YWCA of Kauai Shelter

Illinois
Illinois Coalition Against Domestic Violence

Louisiana
Louisiana Coalition Against Domestic Violence

Maryland
Maryland Network Against Domestic Violence

Massachusetts
A Safe Place, Inc.
Necessities/Necesidades
South Shore Women's Center

Mississippi
The Guardian Shelter

Nevada
Domestic Violence Intervention, Inc.

New Jersey
New Jersey Coalition for Battered Women

North Carolina
North Carolina Coalition Against Domestic Violence

Ohio
Ohio Domestic Violence Network

Rhode Island
Rhode Island Coalition Against Domestic Violence

South Dakota
Crisis Intervention Shelter Service
South Dakota Against Domestic Violence & Sexual Assault
Wholeness Center Family Services

Tennessee
Tennessee Task Force Against Domestic Violence

Texas
Texas Council on Family Violence

Utah
Utah Domestic Violence Advisory Council

Vermont
Vermont Network Against Domestic Violence & Sexual Assault

Virginia
Virginians Against Domestic Violence

West Virginia
West Virginia Against Domestic Violence

Wisconsin
Wisconsin Coalition Against Domestic Violence
Appendix E:

Bibliography
BIBLIOGRAPHY


Dan Browning, Data on School Kids Anything but Private, St. Paul Pioneer Press, March 19, 1995 at 1A.

Dan Browning, Schools Follow Laws, Own Discretion in Releasing Student Data, St. Paul Pioneer Press, Mar. 19, 1995 at 13A.


Robert Davis, Online Medical Records Raise Privacy Fears, USA Today, Mar. 22, 1995, at 1A.


Anonymous Call Rejection, May 1, 1992 (Available from the Bell Atlantic Corporation).

Bell Atlantic IQ Services, June 1991 (Available from the Bell Atlantic Corporation).

Call Block, April 1991 (Available from the Bell Atlantic Corporation).

Caller ID, Feb. 1993 (Available from the Bell Atlantic Corporation).


Lynne A. Marks & Susan H. Rauch, Protecting Confidentiality of Victim-Counselor Communications, 1993 (Available from the National Center on Women and Family Law).

Products and Services, Société Progestacées (Available from Société Progestacées, Montreal, PQ).