

**REPORT OF THE
PRIVACY/PUBLIC RECORDS ACCESS
STUDY COMMITTEE**



OCTOBER 25, 2007



Provided by

GONGWER
NEWS SERVICE, INC.

www.gongwer-oh.com

INTRODUCTION

The Ohio Privacy/Public Records Access Study Committee consists of 23 members appointed by the President of the Senate, the Speaker of the House, the Governor, and the Chief Justice of the Supreme Court.

STRUCTURE & ENABLING LANGUAGE

The Study Committee was created by the 125th General Assembly in Substitute House Bill 204, introduced by Rep. Larry Wolpert. House Bill 204 was enacted by unanimous votes in both the Ohio Senate and the Ohio House of Representatives. It was signed into law on August 5, 2004, by Governor Taft and took effect on November 5, 2004. Section 4(B) directs the committee to study all of the following:

- (1) The concerns associated with the dissemination of personal information contained in public records, including, but not limited to, identity theft, misuse, harassment, and fraud;
- (2) The legitimate uses of personal information contained in public records by businesses, governments, the legal community, and others, including, but not limited to, its use in combating identity theft and fraud;
- (3) The costs to state and local governments associated with placing restrictions on access to personal information contained in public records;
- (4) The impact, including costs, on legitimate businesses, law enforcement, the legal community, government agencies, and others of access restrictions placed on personal information contained in public records;
- (5) The impact of protecting the disclosure of personal information contained in public records through the sealing of documents by court rule;
- (6) Electronic, internet, and bulk access to personal information contained in public records;
- (7) Current and potential future misuse, fraud, harassment, and identify theft prevention and detection efforts, including programs to educate the public on ways to avoid becoming victims, as well as procedures to streamline recovery;
- (8) Existing criminal and civil penalties for misuse of personal information contained in public records and an examination of whether those penalties should be increased as a deterrent.

The bill calls upon the Committee to develop a unified approach to preventing theft, fraud, and the misuse of personal information contained in public records while maintaining access to public records for lawful purposes. The Committee is to consult with the Supreme Court Advisory Committee on Technology and Courts on this endeavor, and to use that body's recommendations as a guide.¹

The Committee is directed to submit a report of its findings to the Senate President, Speaker of the House, Minority Leader of the Senate, Minority Leader of the House of Representatives, the

¹ http://www.sconet.state.oh.us/actc/SGR/Privacy_Report.pdf

Governor, and the Chief Justice of the Supreme Court not later than 12 months after the appointment of all the members of the committee.

COMMITTEE MEMBERS

Representative Larry Wolpert Co-Chairman	Senator David Goodman Co-Chairman
Representative Scott Oelslager	Senator Kevin Coughlin
Representative William Healy	Senator Tom Roberts
Resigned – open seat <i>Local elected official with responsibility for public records</i>	Gordon Gough <i>Representing the credit industry</i>
Deborah Archie <i>Ohio Historical Society/Records Information Management System Administrator from the Department of Administrative Services</i>	John C. Greiner <i>Attorney in private practice specializing in public records law</i>
Roger Blair <i>Representing the financial services industry</i>	Thomas Griesdorn <i>Representing the broadcasting industry</i>
Angela Bosworth <i>Representing information services companies</i>	Steve Hollon <i>Representative of the judicial branch</i>
Michael Chillinsky <i>Representing the legal records industry</i>	Lauren Lubow <i>Attorney from Attorney General's office who specializes in public records law</i>
John Crenshaw <i>Representing the media Clear Channel</i>	Larry Obhof <i>Public Member</i>
Mark Drum <i>Representing law enforcement agencies</i>	Margaret Rittenour <i>Representing realtors</i>
John Fitts <i>Representing the insurance industry</i>	Brad Tillson <i>Representing the newspaper industry</i>
Resigned – Open Seat <i>Consumer advocate</i>	

HEARINGS AND TESTIMONY

The Committee convened on **June 8, 2006** for organizational purposes. The charge of the Committee was read and the members of the Committee introduced themselves. The Committee discussed objectives, topics of study, possible speakers and goals.

On **August 9, 2006**, the Committee heard testimony from representatives of the Legislative Service Commission, who provided the Committee with an overview of current public records law and identity theft statutes. In addition, Jonathan Bowman, Sr. Deputy Attorney General with Crime Victim Services in the Ohio Attorney General's Office, gave a presentation on identify theft and services for victims, including Ohio's nationally recognized PASSPORT program.

During the Committee's meeting on **September 20, 2006**, Bernie Quilter testified on behalf of the Ohio Clerk of Courts Association. Also, Dan Massey, representing the County Recorders' Association, spoke about recently passed legislation that prohibited documents filed with the County Recorder's office from containing Social Security Numbers and legal concerns related to altering existing public records. Jill Thompson, the Athens County Auditor representing the County Auditors' Association, shared her group's concerns with recently passed public records law.

On **October 19, 2006**, John Gilchrist, Director of the Ohio Association of Chiefs of Police, offered testimony on behalf of his group. Lieutenant Timothy Becker with the Columbus Division of Police offered testimony. Sheriff Vernon Stanforth testified on behalf of the Buckeye Sheriffs' Association. Each presented concerns about existing public records laws and how these laws affect the safety of law enforcement officers.

Frank Deaner testified on **November 16, 2006** on behalf of the Ohio Newspaper Association. During this testimony, Mr. Deaner encouraged the Committee to focus on identity theft and posting of public records, rather than redefining public records or expanding exemptions to public records law. Mike Curtain, Associate Publisher of the *Columbus Dispatch*, spoke in support of maintaining access to public records. Edward Esposito, Regional Director of the Radio Television News Directors Association, testified to the importance of public records law in exposing wrongdoing and holding public officials accountable.

During the Committee's meeting on **April 26, 2007**, Sol Bermann, Chief Privacy Officer for the State of Ohio and Co-Chair of the Supreme Court of Ohio's Privacy & Public Access Study Committee, provided an overview of the Subcommittee's recommendations to the Ohio Supreme Court. Basically, members of the Subcommittee reviewed all materials typically found in a court file and identified those containing sensitive data elements – information that might facilitate identity theft.² Members of the Subcommittee then reviewed each data element and voted on

² Recommendation and Report of the Privacy and Public Access Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts on Public Access to Records Maintained by the Ohio Courts – page 8.

whether each should be redacted before public disclosure.³ The report enumerates the information the Subcommittee believed should be exempt from public access.⁴

Sharon Montgomery, Records Administrator for the City of Gahanna, also offered personal testimony during the meeting on April 26, 2007.

Finally, on **May 31, 2007**, Betsy Broder, Assistant Director for the Division of Privacy and Identity Protection for the Federal Trade Commission (FTC), testified about the nature and scope of identity theft, the work of the President's Identity Theft Task Force, and specific issues concerning the protection of personal information held by government entities.

Ms. Broder's testimony said identity theft falls into one of two broad categories: the misuse of existing financial account information and the use of stolen personal information to open new accounts in a consumer's name. While identity thieves obtain information from many sources, public entities play a "critical role in guarding against misuse and unauthorized disclosure of the personal information they collect and maintain." Both Ms. Broder's testimony and the President's Task Force outline the critical role of Social Security numbers and the value of these numbers to identity thieves as the key piece of information used to perpetrate new account fraud. However, they are widely used for legitimate purposes by both public and private entities. The challenge is to find the proper balance to keep this information out of the hands of thieves, while giving legitimate users sufficient means to identify individuals.

³ *Id.*

⁴ Recommendation and Report of the Privacy and Public Access Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts on Public Access to Records Maintained by the Ohio Courts - Section 4.50.

COMMENTS AND RECOMMENDATIONS

Overview

A study by the Federal Trade Commission estimates that 10 million Americans were victims of some form of identity theft in 2003. More than 7,000 cases were reported in Ohio in 2005; and the real danger is that many victims may not be aware that their identity has been stolen until years later, often when they apply for loans and learn that their credit has been compromised. Then, they must spend significant time and money trying to restore their good credit.

The General Assembly has been very proactive in passing strong laws to punish those who engage in identity theft and to help victims recover from identity theft by enacting programs like the PASSPORT program. Prior to 1999, Ohio did not have a specific criminal offense for taking the identity of another, but the General Assembly passed a bill that established minimum penalties for identity theft as a first-degree misdemeanor and based the determination of more serious offenses on the amount of damages suffered by the victim. This was later enhanced in 2002, when the General Assembly passed a bill to better define the crime as intentionally using another person's identifying information to fraudulently obtain credit, property or services.

In 2005, the General Assembly established the Identity Theft Passport Program in the office of the Attorney General, which provides that once a person has filed a report with law enforcement that they have been a victim of identity theft, they may apply for a passport. This official documentation helps them demonstrate their credit-worthiness to creditors and others who may question them as a result of the damage caused by an identity thief. In the first two years of the program, more than 600 passports were issued to victims.

Last General Assembly, in an effort to help consumers stop identity theft before it begins, legislation was enacted that requires any state agency, business or individual that maintains computerized data of personal information to disclose to consumers within 45 days if that personal information has been compromised. To ensure timely disclosure, the bill gave the Ohio Attorney General the authority to bring civil actions against companies in and out of Ohio and provided for fees of up to \$10,000 per day for those found in violation of the law.

In addition, the General Assembly recently passed legislation to better facilitate access to public records in Ohio. House Bill 9 more clearly outlines the process government agencies must follow when responding to public records requests. In addition, it requires elected officials, or their designees, to attend three hours of public records training during their term in office. This training will be developed by the Attorney General and made available free of charge.

House Bill 9 also provides for greater accountability when public offices fail to properly respond to public records requests. If a public office does not properly respond, statutory damages are available to the requestor of up to \$100 a day, and no more than \$1000. In addition, in cases where public offices completely ignore a request, people seeking public records will be able to receive attorneys' fees if they are forced to go to court simply to get a response to their request.

With technology developing the way it has and with more information available on the Internet, the concern for protecting the privacy of individuals has grown dramatically. Hence, there is more work to be done. Public offices collect sensitive personal information that can be misused by identity thieves. Yet, a balance must be maintained between protecting personal information and allowing access to public records. Excessive restrictions could have a detrimental impact on important public purposes such as criminal law enforcement and anti-fraud efforts. In addition, businesses and news organizations must have sufficient means to identify individuals.

Over the course of seven meetings from June 2006 – May 2007, the committee heard testimony from a variety of sources about these issues, including law enforcement, the media and local government representatives. The following comments and recommendations are offered as guidelines for the Ohio General Assembly and other government agencies when considering policies and proposals to help prevent identity theft and maintain access to public records.

Comments and Recommendations

Ohioans must have a means to evaluate government's effectiveness. Access to public records law is traditionally viewed as one of these means. Public records document the operation of public offices, activities supervised or regulated by public offices and activities facilitated by public offices. Access to public records must be maintained and balanced against the need to protect personal information.

Recommendation: Government agencies should seek to maintain, and not restrict, broad access to public records.

The committee recognizes that new forms of technology and communication have and will continue to evolve. Use of electronic communication (e-mail), personal data assistants and communication devices and computers to conduct public business has increased. As new technology helps governments perform more efficiently, it is important to maintain access to public records created with these means.

Recommendation: Electronic communications and other communications through new technologies used in the course of public business should be treated consistently under existing public records laws and court decisions.

With identity theft on the rise, protecting personal information that is included in public records must also be considered. Reducing the opportunity for thieves to obtain personal information is the first step in reducing identity theft. Public and private entities all play a role. Diminishing unnecessary inclusion of Social Security numbers in public documents should be considered.

Recommendation: Review whether it is necessary to include Social Security numbers on public documents and prohibit inclusion if there is no legal significance or legitimate public purpose.

Testimony provided to the committee indicated it is uncommon for identity thieves to go to public offices and request public records for the purposes of obtaining personal information to

commit identity theft. However, while the Internet is a valuable tool for providing access to public records, making Social Security numbers and other financial account numbers available to the general public via the Internet presents the greatest risk.

Recommendation: Government agencies should further seek to expand access to public records by making them easily accessible to the general public on the Internet, *as long as* appropriate steps are taken to redact or truncate Social Security numbers, state and federal identification numbers and other financial account information. However, legitimate government, business and news gathering uses should not be hindered. Therefore, a process should be established that recognizes information may need to be shared for these purposes.

Recommendation: For records not made available on the Internet, government agencies should establish security procedures for protecting personal information from improper disclosure, including procedures for retention and destruction of records. When there is a security breach, affected consumers should be notified in a timely manner in accordance with Ohio law.

ATTACHMENTS

Attachment #1: Recommendation and Report of the Privacy and Public Access Subcommittee of the Supreme Court of Ohio Advisory Committee on Technology and the Courts on Public Access to Records Maintained by the Ohio Courts.

Addendum #2: Further comments and recommendations from individual members of the committee are provided.

Etc.