



Wisconsin Briefs

from the Legislative Reference Bureau



Brief 08-9

July 2008

PRIVACY LAWS IN WISCONSIN

INTRODUCTION

The multiple inadvertent disclosures of clients' social security numbers by state agencies or contractors since December 2006 have heightened concern about the privacy and security of sensitive personal information in the control of government offices. Because publicly revealing persons' social security numbers or other information could lead to identity theft, the state and contractors agreed to offer free credit monitoring to affected persons to alert them to possible financial fraud activity.

On April 15, 2008, Governor Jim Doyle directed state agencies to take steps to improve the protection of the personally identifiable information that is collected by state government officials. As part of this effort, he initiated the appointment of a privacy officer in each agency to be responsible for privacy protection programs.

During the 2007-08 session, the Wisconsin Legislature enacted several laws, and considered others, relating to privacy. This brief summarizes those laws, as well as existing privacy legislation.

THE RIGHT OF PRIVACY

A right to personal privacy is not specifically mentioned in either the federal or state constitutions. However, the U.S. Supreme Court in 1965 acknowledged a right to privacy in *Griswold v. Connecticut* (381 U.S. 479), and several constitutional provisions have been asserted as implicitly recognizing privacy, such as the fourth amendment's "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable

searches and seizures" (mirrored in Article I, Section 11 of the Wisconsin Constitution), and the "due process of law" clauses in the fifth and fourteenth amendments. The concept was eloquently phrased by federal Justice Louis Brandeis in his famous dissent as "the right to be let alone," which he is quoted as regarding as "the most comprehensive of rights and the right most valued by civilized men."

Statutory Right of Privacy. Section 995.50, created by Chapter 176, Laws of 1977, specifically states, "The right of privacy is recognized in this state." Under this law, a person whose privacy has been unreasonably invaded may sue for compensatory damages and attorney's fees, and may seek a court order to prevent such a violation. The law is to be interpreted in accordance with the developing common law of privacy, and it is not to infringe on constitutionally protected communications, either private speech or public news media. "Invasion of privacy" is defined to mean any of the following:

- Intrusion upon the privacy of another of a nature highly offensive to a reasonable person, in a place that a reasonable person would consider private or in a manner which is actionable for trespass.
- The use, for advertising purposes or for purposes of trade, of the name, portrait or picture of any living person, without having first obtained the written consent of the person or, if the person is a minor, of his or her parent or guardian.
- Publicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person, if the defendant has acted either unreasonably or recklessly as to whether there was a legitimate public

interest in the matter involved, or with actual knowledge that none existed. It is not an invasion of privacy to communicate any information available to the public as a matter of public record.

- Conduct that is prohibited under s. 942.09 [representations depicting nudity], regardless of whether there has been a criminal action related to the conduct, and regardless of the outcome of the criminal action, if there has been a criminal action related to the conduct.

2007 LEGISLATIVE ACTIVITY

The 2007 Wisconsin Legislature passed two laws, and considered a number of other proposals, relating to the protection of privacy. Legislation enacted:

- **2007 Wisconsin Act 118.** Prohibits someone from intentionally capturing a visual image of a nude or partially nude person in a locker room or exhibiting, distributing, transmitting, or broadcasting the image from the locker room. It also requires locker room operators to adopt written policies regarding who may enter and remain in the locker room for interviews and what recording devices are allowed to be used.
- **2007 Wisconsin Act 198.** Prohibits a person from looking into another person's residence from a common area in a multiunit dwelling or condominium. This is an enhancement to current law which bans a person from entering another person's private property without consent and looking into a dwelling unit for the purpose of sexual gratification.

Bills that failed to pass:

- Assembly Bill 11 proposed generally prohibiting retailers from requesting that a customer disclose a social security number (SSN) unless required in issuing Department of Natural Resources (DNR) licenses.
- AB-102 proposed prohibiting use of SSNs on state civil service examinations, also banned retailers from requesting customer SSNs, limited the posting of personal information in government records on the Inter-

net, restricted access to certain public and employer records containing SSNs, and prohibited a register of deeds from recording instruments that contain more than a partial SSN.

- AB-316 proposed prohibiting insurers from using SSNs as personal identifiers.
- AB-418 proposed limiting public access to the Wisconsin Circuit Court Access (WCCA) Internet Web site.
- AB-487 proposed authorizing a court to order a person to register with the Department of Corrections as a sex offender if convicted of "video voyeurism," which is making, possessing, or reproducing a visual representation of a person's nudity without consent if the person has a reasonable expectation of privacy.
- AB-533 proposed generally limiting employer monitoring of e-mail messages.
- AB-771 and SB-552 proposed generally prohibiting the state or local governments from using SSNs as identifiers in public records unless authorized or required by state or federal laws or regulations.
- AB-754 and SB-458 proposed removal from WCCA of dismissed cases or charges, cases overturned on appeal, and cases in which the defendant is found not guilty.
- AB-676 was vetoed. It proposed expanding access by certain government agencies to juvenile court records without a court order. Governor Doyle's veto message stated that "it is too broad and would undo significant protections concerning the confidentiality of sensitive information regarding children."

STATE RECORDS PRIVACY INITIATIVE

Social Security Number Incidents. A large accidental release of social security numbers by state government occurred in January 2008. Department of Health and Family Services contractor EDS mailed more than 260,000 brochures to Medicaid clients that mistakenly included their social security numbers on the mailing labels. Later that month, the Depart-

ment of Revenue (DOR) sent a batch of about 5,000 tax forms to northeastern Wisconsin residents, some of which had been improperly folded so as to reveal social security numbers through a window in the mailing envelope. Previously, in December 2006, DOR sent a mailing to more than 170,000 residents that displayed social security numbers on the address labels. Affected individuals have been offered free credit monitoring to help prevent identity theft. In another incident, it was discovered in November 2007 that about 200 University of Wisconsin-Madison employees' university identification numbers, which are based on social security numbers, were displayed for about a year on a Web site that could be seen by the public.

Governor Initiates Agency Privacy Efforts. In response to the information security lapses, Governor Doyle in January 2008 asked the Metavante Corporation to review the state's policies and procedures for protecting sensitive personal information and suggest improvements. Metavante, a company headquartered in Milwaukee with expertise in financial services and privacy protection, agreed to perform the services without cost to the state.

In addition to Metavante's efforts, the governor ordered state executive branch agencies to perform self-assessments regarding the status of protection of sensitive information. The internal audits, which were released on April 14, listed the confidential information agencies hold, how and where it is maintained, and identified vulnerabilities in how it is secured. Significant portions of the reports were blacked out to make sure sensitive personal information and details about agency procedures didn't become known to hackers and identity thieves, according to the Department of Administration's (DOA) chief legal counsel.

On April 14, Metavante issued a report of its investigation and offered ideas regarding better practices to help the state safeguard per-

sonal information. Based on Metavante's assessment and recommendations for improved practices, Governor Doyle on April 15 directed DOA Secretary Michael Morgan to work with all state agencies to develop a plan to implement the following recommendations:

- Replace social security numbers with randomly generated ID numbers wherever possible and as quickly as possible. (State or federal law requires SSNs to be used in some situations for reporting purposes.)
- Appoint a privacy officer in each agency to be responsible for the oversight of their agency's program to protect sensitive information. At the time, only the Department of Revenue had a formalized privacy office with a designated privacy officer charged with accountability for privacy protection.
- Conduct annual risk assessments of each agency's policies and practices for protecting sensitive data.
- Provide a training program for state employees on their roles and responsibilities in protecting sensitive information.
- Develop standardized vendor contract language and due diligence processes which specifically address issues relating to the protection of sensitive information.

The DOA privacy officer will be responsible for coordinating the efforts of agencies' privacy officers to establish consistency in privacy protection programs.

A forerunner of the current initiative was the state Privacy Council and state privacy advocate. Both were created by the 1991 biennial budget [1991 Wisconsin Act 39; Section 15.107 (13), Wisconsin Statutes]. The Privacy Council was authorized to recommend legislation to protect individual privacy and advised the privacy advocate, which it appointed, on rules relating to the collection and use of personal information in computer databases and the right of the individual to inspect, copy, and challenge information accuracy. The council consisted of four members nominated by legislative leaders, one member nominated by the

chief justice of the supreme court, and four other gubernatorial appointees. The privacy advocate, an unclassified state employee, was charged with promoting policies to protect individual privacy, educating people about their rights, assisting individuals in obtaining and challenging data on state computer files, and recommending changes in laws governing the collection of personal information. The council and the advocate were eliminated by 1995 Wisconsin Act 27.

SUMMARY OF OTHER PRIVACY LAWS

Wisconsin has enacted numerous laws relating to the privacy and confidentiality, use and misuse, of personal data in both private and government records. What constitutes “personally identifiable information” is specified in some of the laws, but a general definition in Section 19.62, Wisconsin Statutes, is “information that can be associated with a particular individual through one or more identifiers or other information or circumstances.” Following are summaries of selected statutes of general interest.

Identity Theft. A person may not misappropriate another person’s documents, identification cards, or personal identifying information to obtain or try to obtain credit, money, goods, services, employment, or other things of value or benefit. A person may also not use such information or identification to avoid civil or criminal process or penalty, or cause harm to the reputation, property, person, or estate of the other person. Violation is a Class H felony.

Personal identifying information includes a person’s name, address, telephone number, driver’s license number, social security number, name of employer or place of employment, employment identification number, maiden name of the individual’s mother, taxpayer identification number, a financial depository account number or access number, DNA profile, biometric data (fingerprint, voice print,

retina or iris image), or any other information that is unique to or can be associated with a particular individual.

If an individual reports to a law enforcement agency for the jurisdiction in which he or she resides that personal identifying information or a personal identifying document belonging to the individual appears to be illegally in the possession of another or that another has illegally used or has attempted to illegally use it, the agency must prepare a report on the alleged violation. If the law enforcement agency concludes that it appears not to have jurisdiction to investigate the violation, it must inform the individual of which law enforcement agency may have jurisdiction. [s. 943.201]

Invasion of Privacy. A person may not look into, or use a surveillance device to look into, another person’s dwelling, private property, or private portion of a public accommodation with the intent to observe a nude or partially nude person without the consent of the person being observed, if the observed person has a reasonable expectation of privacy. The law particularly applies to incidents for the purpose of sexual arousal or gratification. [Class A misdemeanor; s. 942.08]

Representations Depicting Nudity (“video voyeurism”). A person may not make, reproduce, or distribute a visual representation that depicts a nude person without the person’s consent if the person has a reasonable expectation of privacy. The crime is a Class I felony. Reproducing or possessing such visual representations is also prohibited. [s. 942.09]

Locker Room Nudity and Policies. While in a locker room, a person, such as a news reporter, may not intentionally depict a nude or partially nude person through a photograph, motion picture, or other means, and may not exhibit, distribute, transmit, or broadcast the image from the locker room. Locker room operators must adopt written

policies regarding who may be present in the locker room to interview or seek information and what cameras or other devices may be used. [s. 942.09]

Opening Letters. Opening someone else's sealed letter or publishing any of its contents is a Class A misdemeanor. [s. 942.05]

Public Library Records. Public library records, such as those documenting what items a patron has borrowed, may generally not be disclosed. An exception is that a law enforcement officer may gain access to records produced by a surveillance device if the officer is investigating criminal conduct alleged to have occurred at the library. [s. 43.30]

Privacy of State-collected Personal Information. Persons applying for licenses and credentials from the Departments of Transportation (DOT), Natural Resources (DNR), and Regulation and Licensing (DRL) must be given the option to restrict the release of certain personal information. An applicant may choose to keep personal data from being sold or provided in lists of 10 or more records to mass marketers and others by specifying on the application form his or her wish to be excluded from bulk lists. This "opt-out" law is designed to reduce unwanted or unsolicited mass mailings or telemarketing calls. Personal identifiers that may be excluded include: name, social security number, telephone number, street address, post office box number, and 9-digit extended ZIP Code. Personal data obtained in batches of 10 or fewer names may still be provided, even if the list includes individuals who opted out of bulk lists. DOT records covered by the law include: driver's (operator's) licenses, motor vehicle registrations, vehicle certificates of title, state identification cards, and special identification cards issued to physically disabled persons for parking. DNR records include: hunting, fishing, trapping, boating, and snowmobile licenses and lists of subscribers to departmental magazines or other publications. DRL records include pro-

fessional or occupational licenses or credentials. [ss. 23.45, 85.103, 440.14]

Income Tax Confidentiality. Employees of DOR may generally not divulge personal information contained on tax returns. An exception is that the net tax for an individual may be disclosed pursuant to an open records request, but the taxpayer will be notified that someone has requested their information. DOR employees are also prohibited from browsing tax records if not required to perform official duties, with violation being grounds for dismissal. If browsing is discovered, the taxpayer is notified and may bring a civil suit for damages. [s. 71.78]

Government Agencies' Personal Information Practices. State and local government officials and agencies must develop rules of conduct and security policies for employees involved in collecting, maintaining, using, providing access to, sharing, or archiving personally identifiable information. Employees must be instructed regarding their duties and responsibilities relating to protecting personal privacy. An agency must try to verify any personally identifiable information it collects from a third party if the information could affect an individual's rights, benefits, or privileges. An agency may not use its Web site to collect personally identifiable information without the user's consent. Employees who violate policies are subject to discipline including suspension without pay or discharge and civil forfeitures of up to \$500 for each violation.

An agency may not sell or rent a record containing an individual's name or address of residence, unless specifically authorized by statute. The attorney general must annually make publicly available a summary of case law and attorney general opinions relating to legal issues regarding governmental collection of personally identifiable information.

Personal information in government employee personnel records is generally not

made available for public inspection. Before an agency releases information from employee personnel records relating to disciplinary action, the employee must be notified and has the option of seeking a court order to stop the disclosure.

Unless a job applicant is one of the finalists (top five) for a position in government employment, a candidate may request confidentiality.

A person may challenge the accuracy of information pertaining to them in a public record. If the agency does not correct the information, it must state the reasons for the denial and allow the person to file a statement in the file stating why they disagree with the disputed portion. [Subch. IV of Ch. 19]

The Public Records Board is required to ensure that state agencies are not maintaining any secret records series containing personally identifiable information and it must facilitate individuals being able to learn if agency records contain such information. [s. 16.61]

The Department of Employee Trust Funds may generally not publicly release personal information relating to individual participants, annuitants, or beneficiaries. [s. 40.07]

The Department of Veterans Affairs may generally not share veterans' separation documents and other papers in its possession, or provide information in those documents to unauthorized persons. [s. 45.04]

The legislative Joint Committee on Information Policy and Technology is tasked to review information management and technology systems, plans, practices, and policies of state and local units of government, including their data security and integrity and their protection of the personal privacy of individuals who are included in databases of state and local government agencies. [s. 13.58]

DOA must ensure that state data processing facilities develop appropriate privacy and information security procedures and safeguards. [ss. 16.971, 16.973]

The state registrar or local registrars may not disclose to unauthorized persons personal information from vital records such as certificates documenting births, marriages, divorces, and deaths. Exceptions are for statistical, administrative, or research uses in which specific individuals cannot be identified. [s. 69.20]

Notice of Unauthorized Acquisition of Personal Information. If a business or state or local government agency knows that personal information in the entity's possession has been acquired by an unauthorized person, the entity must generally make reasonable efforts to notify each subject affected. Information covered includes a person's name if linked to a social security number, driver's license number, state identification number, financial account information, DNA profile, unique biometric data, or any other unique physical representation. If a single incident requires the notification of 1,000 or more persons, the entity must also notify all consumer reporting agencies about the situation. Notice is not required if the acquisition of personal information does not create a material risk of identity theft or fraud or if the personal information was acquired in good faith by the entity and used for a lawful purpose. [s. 134.98, renumbered from s. 895.507 by 2007 Wisconsin Act 97, a Revisor's correction bill]

"Dumpster Diving" – Disposal of Business Records. A financial institution, medical business, or tax preparation business may not dispose of a record containing personal information unless it properly disposes of it by shredding the record, erasing the personal information contained in the record, modifying the record to make the personal information unreadable, or taking action that it reasonably believes will prevent unauthorized persons from having access to the personal information in the record for the period between the record's disposal and the record's destruction. Personal information covered includes data about an individual's medical

condition, financial account information, or personally identifiable data relating to tax returns. A violator may be subject to lawsuits for damages and civil forfeitures of up to \$1,000. A person who uses personal information that was disposed of by a business is liable for damages and may also be criminally prosecuted with a penalty of a fine of not more than \$1,000 or 90 days' imprisonment, or both. [s. 134.97 (2)]

Telecommunications Privacy. Except as ordered by a court, a person may generally not intercept, record, disclose, or otherwise use without authorization another person's private communications, whether the communications are conducted by wire, electronically, or verbally. Violation is a Class H felony, and violators may be liable in a civil action for actual damages between \$100 and \$1,000 per day, punitive damages, and reasonable attorney's fees and other litigation costs. Employers may monitor telephone and electronic mail communications on systems they control for quality control purposes. An individual may record a conversation to which he or she is a party without the consent of any other party to the conversation. [s. 968.31]

Unless a subscriber to a cable television service has given written consent within the preceding two years, another person may not monitor the subscriber's equipment, or the use of it, except to verify the system's integrity or to collect information for billing of pay services. A cable television provider may also not provide anyone with the name or address or other information that discloses or reasonably leads to the disclosure of any aspect of the subscriber's household's behavior, such as viewing habits or preferences. A victim of an intrusion of privacy under this law may sue for compensatory damages and attorney's fees, and may seek a court order to prevent the breach of privacy. [s. 134.43]

The Public Service Commission (PSC) must establish privacy guidelines applicable

to telecommunications services and review and revise them every two years. A telecommunications provider introducing a new service must explicitly address privacy considerations. The PSC appoints a Telecommunications Privacy Council consisting of representatives of telecommunications providers and consumers of telecommunications services (including the state). The council advises the PSC concerning administration of the law and the content of rules promulgated under the law. [s. 196.209]

Notary Public Confidentiality. A notary public must keep confidential all documents and information contained in documents reviewed by the notary while performing official duties and may not release the documents or the information to a third person without written consent. [s. 137.01 (5m) (a)]

Employment and Insurance Privacy. An employer may not make any inquiries to a prospective employee that in any way imply or express that a prohibited basis of discrimination may be a consideration in hiring. Similar discriminatory limitations may not be included in the application form or mentioned in job advertisements. Among the topics that may not be brought up by the employer are ancestry, age, arrest or conviction record, sexual orientation, marital status, or use of lawful products (such as tobacco) off the work-site during nonworking hours. [s. 111.322 (2)]

Employers may generally not ask or require prospective or current employees to submit to an honesty testing device ("lie detector" or polygraph machine, or voice stress analyzer). Excepted are investigations relating to theft, embezzlement, or other crimes, if the employee had access to the missing property and there is reasonable suspicion of involvement in the crime. [ss. 111.37, 942.06]

An employer may not solicit, require, or administer a genetic (DNA) test as a condition of employment. Excepted are DNA tests with

the employer's informed consent for the purposes of investigating a worker's compensation claim or determining the worker's susceptibility or exposure to potentially toxic workplace chemicals or substances. [ss. 111.372, 942.07]

Health and medical care insurers may not request DNA tests, use the results of tests, or consider a refusal to obtain a test, as a basis for determining whether to insure a person or in setting rates. Excepted are companies writing life insurance or income continuation insurance policies. [s. 631.89]

Employers may generally not ask or require employees to submit to a test for the HIV virus (which may lead to AIDS), and may not use the results of such a test to affect a person's employment. [s. 103.15]

Health Care Privacy. Health care providers must maintain the confidentiality of patient health care records and may not disclose medical records to unauthorized parties. A violator may be liable for actual money damages, exemplary damages, and legal costs. [ss. 146.81 to 146.84, 146.50]

Managers of nursing homes and similar care facilities must protect and promote the privacy rights of residents. These rights include privacy regarding accommodations, medical treatment, written and telephonic communications, visits, and meetings of family and of resident groups, and confidentiality of personal and clinical records. [ss. 49.498, 50.09]

A person may not obtain confidential patient records regarding a person's mental health care under false pretenses or disclose confidential information knowing it is unlawful to do so and is not reasonably necessary to protect another from harm. A violator may be fined not more than \$25,000 or imprisoned not more than 9 months, or both. A person may not negligently disclose confidential mental

health treatment information. The penalty is a forfeiture of not more than \$1,000 for each violation. A person may not intentionally disclose confidential mental health information for pecuniary gain. A violator may be fined not more than \$100,000 or imprisoned not more than 3 years and 6 months, or both. [s. 51.30 (10)]

Abortion Privacy. Prior to undergoing an abortion, a woman must give voluntary and informed written consent. She must be offered certain explanatory printed materials and private counseling in an individual setting that protects her privacy and maintains the confidentiality of her decision. [s. 253.10 (3)]

Children's Privacy. The records relating to law enforcement and court proceedings of juveniles, as well as adult expectant mothers of unborn children, must be kept separate from the records of adults and are generally not made available for inspection under the open records law. News media may report information from these records if identities are not revealed. [s. 48.396 (1)]

Public school pupil records are confidential, and school boards must adopt regulations to protect the confidentiality of records relating to a student's progress, behavior, health, and other data. Exceptions are provided for law enforcement situations and legal procedures. [s. 118.125 (2) (k)]

A pupil's communications with a school's psychologist, counselor, social worker, and nurse, and a teacher or administrator who engages in alcohol or drug abuse program activities regarding the pupil's substance use, is privileged and confidential and may not be disclosed. Excepted are situations such as if there is reason to believe that there is serious and imminent danger to the health, safety, or life of any person and that disclosure of the information to another person will alleviate the danger. [s. 118.126]