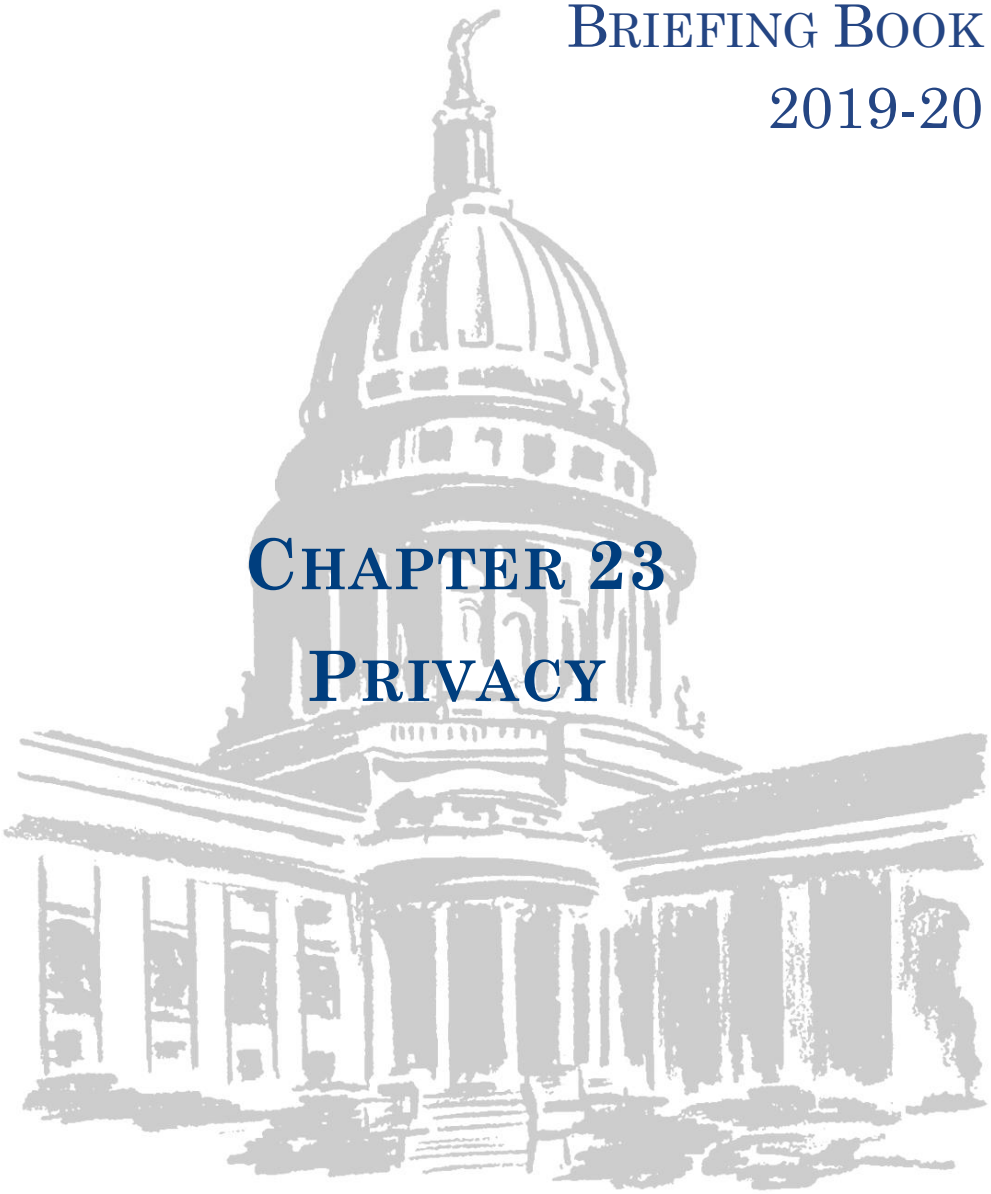
Wisconsin Legislator Briefing Book 2019-20



Chapter 23
Privacy

Dan Schmidt, Principal Analyst
Wisconsin Legislative Council

Table of Contents

Copies of the Wisconsin Legislator Briefing Book are available at:
http://www.legis.wisconsin.gov/lc

Introduction

In Wisconsin, there is no specific state agency with general responsibility for privacy. Instead, the state relies on a number of privacy laws that are generally enforced privately in the case of civil violations or by local district attorneys in the case of criminal violations.

The laws described in this chapter are the major privacy provisions in the Wisconsin statutes. While it is not an exhaustive list, it includes significant privacy provisions that are often the subject of constituent questions.

Wisconsin law recognizes the right to privacy and defines when equitable relief, compensatory damages, and attorney fees may be provided if privacy is invaded.

Invasion of Privacy

Civil Action

Wisconsin law recognizes an individual right to privacy. Under the statutes and case law, a person may bring a civil action for damages resulting from an invasion of privacy. For purposes of civil relief, an invasion of privacy is defined as any of the following:

- **Highly Offensive Intrusion on Privacy.** An 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 that is actionable for trespass.
- **Using a Person's Name or Likeness.** 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 About Private Life Events.** 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.
- **Depictions of Nudity.** Conduct involving a representation that depicts nudity without the knowledge and consent of the person who is depicted nude in a circumstance in which the person has a reasonable expectation of privacy, regardless of whether there has been a criminal action related to the conduct or regardless of the outcome of such a criminal action.

However, it is not an invasion of privacy to communicate any information available to the public as a matter of public record.

Under Wisconsin law, a person whose privacy has been invaded is entitled to all of the following remedies:

- Equitable relief to prevent and restrain an invasion of privacy, excluding prior restraint of constitutionally protected speech.

- Compensatory damages based on the plaintiff's loss or the defendant's unjust enrichment, if proven.
- Reasonable attorney fees.

If the court determines that an action for invasion of privacy is frivolous, the court must award the defendant reasonable fees and costs relating to the defense. A frivolous action is an action that was commenced in bad faith or for harassment purposes or an action that was commenced without an arguable basis. [s. 995.50, Stats.]

Crime of Invasion of Privacy

Under Wisconsin law, the following crimes of invasion of privacy are punishable as a Class A misdemeanor:

The crime of invasion of privacy prohibits, among other acts, the use of a surveillance device in a private place if the person has the intent to observe a nude or partially nude individual and does not have the consent of that individual.

- Installing or using a surveillance device in a private place with the intent to observe a nude or partially nude person without the consent of the person observed.
- Looking into, for the purpose of sexual arousal or gratification, a private place that is or is part of a public accommodation (public restrooms, etc.) in which a person may be nude or partially nude, regardless of whether an individual is present or not.
- Entering another person's private property without consent or entering an enclosed or unenclosed common area of a multi-unit dwelling or condominium and viewing an individual who has a reasonable expectation of privacy in that part of the dwelling, without consent, for the purposes of sexual gratification or arousal and with the intent to intrude upon or interfere with the individual's privacy.

An invasion of privacy crime is punishable as a Class I felony in the following circumstances:

- One of the aforementioned misdemeanor invasion of privacy crimes is perpetrated against a person who has not attained the age of 18 at the time of the violation.
- A person knowingly installs or uses any device, instrument, mechanism, or contrivance to intentionally view, broadcast, or record under the outer clothing of an individual that individual's genitals, pubic area, breast, or buttocks, including genitals, pubic area, breasts, or buttocks that are covered by undergarments, or to intentionally view, broadcast, or record a body part of an individual that is not otherwise visible, without that individual's consent.

A person who is convicted of a Class A misdemeanor may be fined up to $10,000, imprisoned for nine months, or both, and a person who is convicted of a Class I felony may be fined up to $10,000, imprisoned for up to three years and six months, or both. The court may also order an individual convicted, adjudicated delinquent, or found not guilty by reason of mental disease or defect to register with the Department of Corrections as a sex offender. [s. 942.08, Stats.]

Personal Internet Account Privacy

Wisconsin law specifies that certain actions by an employer, educational institution, or landlord in accessing a person's personal Internet accounts are prohibited and may be subject to a forfeiture and enforcement by the Department of Workforce Development (DWD). For the purposes of the law, a "personal Internet account" is an Internet-based account that is created and used by an individual exclusively for purposes of personal communications.

Wisconsin law prohibits access to certain personal Internet information by employers, educational institutions, and landlords.

The law explicitly states that its provisions do not create a duty for an employer, educational institution, or landlord to search or monitor the activity of a personal Internet account. Likewise, an employer, educational institution, or landlord is not liable for any failure to request or to require access or observation of a personal Internet account.

Employers

The law specifies that, with certain exceptions, an employer may not request or require an employee or applicant to disclose access information, grant access, or allow observation, of a personal Internet account, as a condition of employment. An employer is also prohibited from discharging or otherwise discriminating against a person who refuses such a request or opposes such practices.

Under the exceptions, an employer may do any of the following:

- Discharge or discipline an employee for transferring proprietary or confidential information, or financial data, to the employee's personal Internet account without authorization.
- Conduct an investigation of certain misconduct, if the employer has reasonable cause to believe that activity in the personal Internet account relating to the misconduct has occurred. Misconduct includes: any alleged unauthorized transfer of proprietary or confidential information, or financial data; any other alleged employment-related misconduct; any violation of the law; or any violation of the employer's work rules as specified in an employee handbook. In conducting an investigation, an employer may require an employee to grant access or allow observation of a personal Internet account, but may not require the employee to disclose access information for that account.
- Restrict or prohibit a person's access to certain Internet sites while using a device or network that is supplied or paid for in whole or in part by the employer.
- Request or require access to a device, account, or service that is supplied or paid for in whole or in part by the employer, which is provided by virtue of the employment relationship or is used for the employer's business purposes.

- View, access, or use information about an employee or applicant that is available in the public domain or that can be viewed without access information.
- Request or require disclosure of an employee's personal email address.

Additionally, the law does not prevent an employer in the securities industry from complying with regulations relating to applicant screening and business oversight.

An employer that inadvertently obtains access information, through use of the employer's network or use of a device that is supplied or paid for in whole or in part by the employer, is not liable for possessing that information so long as the information is not used to access the employee's personal Internet account.

Educational Institutions

The law specifies that, with certain exceptions, an educational institution may not request or require a student or prospective student to disclose access information, grant access, or allow observation, of a personal Internet account, as a condition of admission or enrollment. An educational institution is also prohibited from refusing to admit, expel, suspend, or otherwise discipline a person who refuses such a request or opposes such practices. An "educational institution" includes a college, university, technical college, public school, charter school, private school, and a private educational testing service.

Under the exceptions, an educational institution may request or require access to a device, account, or service that is supplied or paid for in whole or in part by the educational institution, which is provided by virtue of the student's admission to the institution or is used for educational purposes. An educational institution may also view, access, or use information about a student or prospective student that is available in the public domain or that can be viewed without access information.

Landlords

Under Wisconsin law, a landlord may not request or require a tenant or prospective tenant to disclose access information, grant access, or allow observation, of a personal Internet account, as a condition of tenancy. A landlord is also prohibited from discriminating against a tenant or prospective tenant who refuses such a request or opposes such practices. A landlord may view, access, or use information about a tenant or prospective tenant that is available in the public domain or that can be viewed without access information.

An employer, educational institution, or landlord who violates a person's privacy rights in a personal Internet account is subject to a forfeiture of up to $1,000. Additionally, a person who has been discharged, expelled, disciplined, or otherwise discriminated against in violation of the law may file a complaint with DWD, which may take action to remedy the violation in the same manner as employment or housing discrimination complaints.

[s. 995.55, Stats.]

Prohibitions on Representations Depicting Nudity

Wisconsin law prohibits certain representations depicting nudity without the express permission of the subject of the depiction. A representation is generally defined as a photograph, exposed film, motion picture, videotape, recording or other audio or visual representation, or data that represents a visual image or audio recording. An intimate representation is specifically defined as:

- A representation of a nude or partially nude person.
- A representation of clothed, covered, or partially clothed or covered genitalia or buttock that is not otherwise visible to the public.
- A representation of a person urinating, defecating, or using a feminine hygiene product.
- A representation of person engaged in sexual intercourse or sexual contact.

Wisconsin law generally prohibits certain representations depicting nudity without the express permission of the individual depicted in the representation.

Capturing, Reproducing, Possessing

The law provides that anyone who does any of the following may be found guilty of a Class I felony and may be fined up to $10,000, imprisoned for three years and six months, or both:

- Captures an intimate representation without the consent of the person depicted under circumstances in which he or she has a reasonable expectation of privacy, if the person knows or has reason to know that the person who is depicted does not consent to the capture of the intimate representation.
- Makes a reproduction of an intimate representation that the person knows or has reason to know was captured in violation of the above provision and that depicts an intimate representation captured in violation of the above provision, if the person depicted in the reproduction did not consent to the making of the reproduction.
- Possesses, distributes, or exhibits an intimate representation that was captured in violation of the above provision or a reproduction made in violation of the above provision(s), if the person knows or has reason to know that the intimate representation was captured in violation of the above provision or the reproduction was made in violation of the above provision(s), and if the person who is depicted in the intimate representation or reproduction did not consent to the possession, distribution, or exhibition.

A person who violates these prohibitions faces higher penalties if the victim is under 18. However, there are exceptions for parents or guardians and for representations of public importance. If the person depicted in violation of these prohibitions had not, at the time of the violation, attained the age of 18 years, the person who commits a violation may be found guilty of a Class H felony, and may be fined up to $10,000, imprisoned for six years, or both.

[s. 942.09 (2), Stats.]

2017 Wisconsin Act 129 created a new crime that generally prohibits soliciting sexually explicit representations from minors. Specifically, the Act prohibits a person from soliciting an intimate or private representation from a person who the actor believes or has reason to believe is less than 18 years of age. The prohibition created by the Act does not apply to a person who solicits such representations and is less than 18 years of age. The penalty for a violation of this crime is a Class A misdemeanor if the person who solicits the intimate or private representation is at least 18 years of age, but has not attained 21 years of age, and if the child solicited is not more than three years younger than the person who solicited the intimate or private representation. In all other instances, a violation of the prohibition created by the Act by a person who is at least 18 years of age is penalized as a Class I felony.

[s. 942.09 (4), Stats.]

Distribution of Sexually Explicit Images

Wisconsin law prohibits the distribution of certain sexually explicit images without the consent of the person depicted. The statutes specifically prohibit a person from doing the following:

- Posting, publishing, or causing to be posted or published, a private representation if the actor knows that the person depicted does not consent to the posting or publication of the private representation.
- Posting, publishing, or causing to be posted or published, a depiction of a person that he or she knows is a private representation without the consent of the person depicted.

"Posting or publishing" includes posting or publishing on a website, if the website may be viewed by the general public. A "private representation" is defined as a representation depicting a nude or partially nude person or depicting a person engaged in sexually explicit conduct that is intended by the person depicted to be captured, viewed, or possessed only by the person who, with the consent of the person depicted, captured the representation or to whom the person depicted directly and intentionally gave possession of the representation.

A violation of either of these provisions is a Class A misdemeanor, punishable by imprisonment for up to nine months, a fine of up to $10,000, or both. If the person depicted or represented in the violation of this provision had not, at the time of the violation, attained the age of 18 years, the person who commits a violation may be found guilty of a Class I felony and may be fined up to $10,000, imprisoned for up to three years and six months, or both.

This prohibition does not apply to the following:

- The parent, guardian, or legal custodian of the person depicted if the private representation does not violate the crime of sexual exploitation of a child or possession of child pornography, and the posting or publication is not for the purpose of sexual arousal, gratification, humiliation, degradation, or monetary or commercial gain.

- A law enforcement officer or agent, acting in his or her official capacity in connection with the investigation or prosecution of a crime.
- A person who posts or publishes a private representation that is newsworthy or of public importance.
- A provider of an interactive computer service, as defined in 47 U.S.C. s. 230 (f) (2), or to an information service or telecommunications service, as defined in 47 U.S.C. s. 153, if the private representation is provided to the interactive computer service, information service, or telecommunications service by a third party.

[s. 942.09 (3m), Stats.]

Representations Depicting Nudity in a Locker Room

Wisconsin law generally prohibits a person from intentionally capturing, while present in a locker room, a representation of a nude or partially nude person while the person is nude or partially nude in the locker room without permission. Such violations are punishable as a Class A misdemeanor if the victim is an adult, and a violator may be fined up to $10,000, imprisoned for nine months, or both, and as a Class I felony if the person represented in the violation was under 18 years at the time of the violation. This prohibition does not apply if the person consents to the capture of the representation and the person is, or the actor reasonably believes that the person is, 18 years of age or over when the person gives his or her consent, or the person's parent, guardian, or legal custodian consents to the capture of the representation.

Wisconsin law also prohibits, without adult consent, a person from intentionally exhibiting or distributing to another a representation of a nude or partially nude person while the actor is present in, and the person is nude or partially nude in, the locker room, or transmitting or broadcasting an image of a nude or partially nude person from a locker room while the person is nude or partially nude in the locker room. A violation of one of these provisions is a Class I felony, punishable by a fine of up to $10,000, imprisonment for up to three years and six months, or both. If the person represented in the violation had not, at the time of the violation, attained the age of 18 years, the violation is a Class H felony, punishable by a fine of up to $10,000, imprisonment for up to six years, or both.

[s. 942.09, Stats.]

Use of a Drone

Wisconsin law prohibits an individual from using a drone with the intent to photograph, record, or otherwise observe another individual in a place or location where the individual has a reasonable expectation of privacy. The penalty for a violation of this provision is a Class A misdemeanor, punishable by imprisonment for up to nine months, a fine of up to $10,000, or both. This prohibition does not apply to a law enforcement officer authorized to use a drone pursuant to a search warrant.

[s. 942.10, Stats.]

Identity Theft

Identity theft occurs when a person intentionally uses or attempts to use personal identifying information or personal identification documents of another to obtain anything of value, including credit or services.

The unauthorized use of personal identifying information, commonly termed "identity theft," is prohibited in Wisconsin. A person who intentionally uses or attempts to use personal identifying information or personal identification documents (a birth certificate, PIN number, or financial transaction card) of another individual to obtain credit, money, goods, services, or anything of value, without that individual's authorization or consent, to avoid civil or criminal process or penalty, or to harm the reputation, property, person, or estate of an individual, is guilty of a Class H felony. A Class H felony is punishable by imprisonment for up to six years, a fine of up to $10,000, or both.

For the purposes of this statute, personal identifying information includes an individual's:

- Name.
- Address.
- Telephone number.
- Driver's license number.
- Social Security number.
- Employer or place of employment.
- Employee identification number.
- Mother's maiden name.
- Financial account numbers.
- Taxpayer identification number.
- DNA profile.
- Any number or code that can be used alone or with an access device to obtain money, goods, services, or any other thing of value.
- Unique biometric data, including a fingerprint, voice print, retina or iris image, or any other unique physical representation.
- Any other information or data that is unique to, assigned to, or belongs to an individual and that is intended to be used to access services, funds, or benefits of any kind to which the individual is entitled.
- Any other information that can be associated with a particular individual through one or more identifiers or other information or circumstances.

In addition, the law provides that if any individual reports an identity theft violation to the law enforcement agency where the individual resides, but the violation occurs outside of that law enforcement agency's jurisdiction, the law enforcement agency receiving the complaint must prepare a report on the violation and forward it to the law enforcement agency in the appropriate jurisdiction. [s. 943.201, Stats.]

Records Containing Personal Information

Wisconsin law requires certain businesses and government entities to take actions to protect personal information.

Financial institutions, medical businesses, and tax preparation businesses in Wisconsin must make personally identifying information in their documents undiscoverable before disposing of them, and certain businesses must notify individuals of unauthorized acquisition of personal information.

Disposal of Records

Wisconsin law prohibits financial institutions, medical businesses, and tax preparation businesses in this state from disposing of records that contain personal information unless the personal information is first rendered undiscoverable. The statutes provide that these businesses may discard the records only after they do one of the following prior to disposal:

- Shred the records.
- Erase the personal information contained in the records.
- Modify the records to make the personal information unreadable.
- Take actions that the businesses reasonably believe will ensure that no unauthorized individual will have access to the personal information contained in the records prior to their destruction (e.g., locked dumpsters).

For the purposes of this statute, personal information generally includes medical information, account or credit information, account or credit application information, and tax information, by which an individual is capable of being associated through one or more identifiers.

Wisconsin law requires certain business entities to notify individuals of unauthorized acquisitions of personal information. If an entity whose principal place of business is located in Wisconsin or an entity that maintains or licenses personal information in Wisconsin knows that personal information in the entity's possession has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must make reasonable efforts to notify each subject of the personal information. The notice must indicate that the entity knows of the unauthorized acquisition of the personal information. [s. 134.98, Stats.]

A business that improperly disposes of such records may be required to forfeit up to $1,000 per violation and may be held liable for damages to the individual whose personal information was disposed of improperly. A person who uses personal information that was improperly disposed of is also liable for damages and may be fined not more than $1,000, imprisoned for not more than 90 days, or both. Such a violation is commonly referred to as "dumpster diving." [s. 134.97, Stats.]

Notification Requirements

Specified entities must provide notification regarding the unauthorized acquisition of personal information. The law applies to entities that:

Certain business entities must notify individuals of the unauthorized acquisition of personal information held by those entities.

- Conduct business in Wisconsin and maintain personal information in the course of business.
- License personal information in Wisconsin.
- Maintain a depository account for a Wisconsin resident.
- Lend money to a resident of Wisconsin.

An "entity" also includes:

- The state and any office, department, independent agency, authority, institution, association, society, or other body in state government created or authorized to be created by the constitution or any law, including the Legislature and the courts.
- A city, village, town, or county.

For purposes of the notification requirements, "personal information" means an individual's last name and first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in any manner that renders the element unreadable:

- The individual's Social Security number.
- The individual's driver's license number or state identification number.
- The number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account.
- The individual's DNA profile.
- The individual's unique biometric data, including a fingerprint, voice print, retina or iris image, or any other unique physical characteristic.

If an entity whose principal place of business is not located in Wisconsin knows that personal information pertaining to a Wisconsin resident has been acquired by a person whom the entity has not authorized to acquire the personal information, the entity must make reasonable efforts to notify each Wisconsin resident who is the subject of the personal

information. The notice must indicate that the entity knows of the unauthorized acquisition of personal information pertaining to the resident.

If a person, other than an individual, that stores personal information pertaining to a Wisconsin resident, but does not own or license the personal information, knows that the personal information has been acquired by a person whom the person storing the personal information has not authorized to acquire the personal information, and the person storing the personal information has not entered into a contract with the person that owns or licenses the personal information, the person storing the information must notify the person that owns or licenses the information of the acquisition as soon as practicable.

If, as a result of a single incident, an entity is required to notify 1,000 or more individuals that personal information pertaining to the individuals has been acquired, the entity must, without unreasonable delay, notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices sent to the individuals.

An entity is not required to provide notice if: (1) the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information; or (2) the personal information was acquired in good faith by an employee or agent of the entity and the personal information is used for a lawful purpose. [s. 134.98, Stats.]

Timing and Method of Notice

An entity must provide the required notice within a reasonable time, not to exceed 45 days, after the entity learns of the acquisition of personal information. A determination of reasonableness must include consideration of the number of notices that an entity must provide and the methods of communication available to the entity. Notice must be provided by mail or by a method the entity has previously employed to communicate with the subject of the personal information. If an entity cannot with reasonable diligence determine the mailing address of the subject, and if the entity has not previously communicated with the subject, the entity must provide notice by a method reasonably calculated to provide actual notice to the subject. Upon written request by a person who has received a notice, the entity that provided the notice must identify the personal information that was acquired. [s. 134.98 (3), Stats.]

Exemptions

These notice provisions do not apply to financial institutions that are subject to and in compliance with federal law relating to disclosure of nonpublic personal information or to a person that has a contractual obligation to such an entity, if the entity or person has in effect a policy concerning breaches of information security. In addition, the provisions do not apply to health plans, health care clearinghouses, or health care providers, if the entity complies with federal law relating to security and privacy of information maintained by those entities.

In addition, a law enforcement agency may, in order to protect an investigation or homeland security, ask an entity not to provide a notice that is otherwise required for a period of time. The notification process must begin at the end of that time period. If an entity receives such a request, it may not provide notice of or publicize an unauthorized acquisition of personal information, except as authorized by the law enforcement agency that made the request. [s. 134.98 (3m), Stats.]

Privacy of Health Care Records

Wisconsin law requires that all patient health care records remain confidential unless a patient or a person authorized by the patient gives explicit informed consent to the release of the patient's health care record or unless the situation comes within one of the exceptions listed in the law. A patient health care record is defined as any record related to the health of a patient prepared by or under the supervision of a health care provider. [s. 146.82, Stats.]

Patient health care records are generally confidential and may not be disclosed except with the informed consent of the patient or a person authorized by the patient to give consent or under exceptions specified in Wisconsin statutes.

Informed consent to disclose patient health care records to an individual, agency, or organization must be in writing. A statement of informed consent must include all of the following:

- The name of the patient whose record is being disclosed.
- The type of information to be disclosed.
- The types of health care providers making the disclosure.
- The purpose of the disclosure.
- The individual, agency, or organization to which disclosure may be made.
- The signature of the patient or the person authorized by the patient and, if signed by a person authorized by the patient, the relationship of that person to the patient or the authority of the person.
- The date on which the consent is signed.
- The time period during which the consent is effective.

Q: Can I see my own medical records?

A: Yes. A health care provider must allow you to inspect your medical records during regular business hours if you provide reasonable notice of your intent to inspect the records. You may also receive a copy of your health care records; however, the health care provider may charge reasonable costs for providing copies.

In certain circumstances, patient health care records may be released without the informed consent of the patient. These circumstances include release of information to other health care workers who are caring for the patient, government agencies with certain health care responsibilities, and certain health care research organizations. Absent informed consent, recipients of patient health care information generally must keep that information confidential and may not disclose such information.

Violations of the laws on confidentiality of patient health care records are punishable by penalties, with the severity of the penalty varying depending on whether the violation was negligent, intentional, or intentional with a pecuniary gain. Private lawsuits are also authorized, in which a plaintiff may recover actual damages, specified exemplary damages, and costs and attorney fees. [ss. 146.82 and 146.83, Stats.]

Although similar to general patient health care records, the treatment of mental health records and human immunodeficiency virus (HIV) test results is governed by separate statutes. Mental health record laws are set forth in s. 51.30, Stats., and HIV test result laws are set forth in s. 252.15, Stats.

Prohibition on Wiretapping

A person may generally record a communication if the person is a party to the communication or has prior consent from one of the parties to the communication.

Wisconsin law generally prohibits the intentional actual or attempted interception, actual or attempted use of a device to intercept, intentional alteration, and actual or attempted disclosure of information obtained through the interception of wire, electronic, or oral communication. Generally, a person not acting under color of law may intercept wire, electronic, or oral communication, commonly referred to as wiretapping, only if that person is a party to the communication or has prior consent from one of the parties to the communication.

However, a person is strictly prohibited from performing any interception with the purpose of violating a law or committing any other injurious act. A violation of the wiretapping prohibitions is a Class H felony punishable by a fine of up to $10,000, imprisonment for up to six years, or both. [s. 968.31, Stats.]

National Do Not Call Registry

1-888-382-1222
http://www.donotcall.gov

Prohibition on Unauthorized Telephone Solicitations

Residents of Wisconsin who do not wish to receive telephone solicitations may request to be included in the National Do Not Call Registry. The

registry is maintained by the Federal Trade Commission (FTC).

A telephone solicitor (or employee or contractor) may not make a telephone solicitation to a residential customer if that individual is listed in the Do Not Call Registry. A telephone solicitor also may not make a telephone solicitation to a nonresidential customer if the nonresidential customer (e.g., a business) has provided the solicitor with notice by mail that the nonresidential customer does not wish to receive telephone solicitations. Finally, a telephone solicitor may not require an employee or contractor to make a telephone solicitation in violation of the provisions of the nonsolicitation prohibition. These prohibitions do not apply if a telephone solicitation is made in response to the recipient's request for such a solicitation or when the recipient is a current client of the person selling property, goods, or services through telephone solicitation. The nonsolicitation prohibition does not apply to a nonprofit corporation, or its employees or contractors, that engage in telephone solicitation.

In addition, a telephone solicitor may not use a prerecorded message in a telephone solicitation without the consent of the recipient of the solicitation.

A person who violates the telephone solicitation regulations may be required to forfeit $100 per violation. The Department of Agriculture, Trade and Consumer Protection (DATCP) enforces these provisions. [s. 100.52, Stats.]

Q: Can a private company require me to provide my Social Security number as a condition of engaging in business?

A: Yes. Federal law does not prohibit private businesses' use of Social Security numbers for any legitimate purpose. Financial institutions and other creditors often use Social Security numbers as financial identifiers when checking credit histories. You may refuse to provide your Social Security number on such occasions; however, the business making the request is under no obligation to provide goods or services if you refuse.

Social Security Numbers

Use and Collection by Government

Federal law places a number of restrictions on state and local governmental use of an individual's Social Security number. For example, the federal Privacy Act of 1974 generally prohibits federal, state, or local government agencies from denying to an individual any right, benefit, or privilege provided by law because that individual refuses to disclose his or her Social Security number. This prohibition does not apply if: (1) the disclosure is required by federal law or the disclosure is required by a federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975; or (2) the disclosure was required under a statute or regulation adopted prior to that date to verify the identity of an individual.

Federal law also authorizes several specific uses that a state or local government, or an agency thereof, may make of a person's Social Security number. For example, the Social Security Act authorizes states or local units of government to require individuals to disclose their Social Security numbers and to utilize such numbers as a form of identification in the administration of a tax program, a general public assistance program, a driver's license or motor vehicle registration program, or a blood donor program, and in the administration of laws relating to birth certificates.

Federal law limits the circumstances under which a state or local government may request an individual's Social Security number. Federal law also requires the state to collect Social Security numbers as a condition for receiving federal funding for child support and family assistance programs.

While a state or local governmental agency is limited in its ability to require individuals to disclose their Social Security numbers, those agencies are not prohibited from **requesting** that a person provide his or her Social Security number. However, if a state or local governmental agency requests a person to disclose his or her Social Security number under any situation, the federal Privacy Act of 1974 requires the state or local government agency to advise the individual whether the disclosure is mandatory or voluntary, under what statutory authority or other authority the Social Security number is requested, and what uses will be made of the Social Security number.

The federal Personal Responsibility and Work Opportunity Reconciliation Act established a requirement that all states collect Social Security numbers as a condition of receiving federal funding for child support and family assistance programs. These laws were created to assist states and the federal government in finding and reducing the number of individuals evading child support payments. Thus, as a condition of receiving any license in Wisconsin, an individual's Social Security number must be recorded on the license application. Social Security numbers are also required for records relating to a divorce decree, support order, paternity determination, and on death certificates.

Private Collection of Social Security Numbers

While the Social Security number is commonly used as a financial identifier, the federal government does not regulate the collection of Social Security numbers by private individuals or corporations. Certain industries (credit, banking, etc.) may require a Social Security number as a condition of conducting business; however, it is up to the discretion of the individual to decide to release or withhold a Social Security number in private matters.

Additional References

1. National Conference of State Legislatures (NCSL) Telecommunications and Information Technology website at: http://www.ncsl.org/. NCSL publications that are not available on the NCSL website are usually available at no charge to legislators and staff. To order copies, contact the NCSL Publication Department at 303-364-7812.
2. Federal Communications Commission website at: http://www.fcc.gov/.
3. Office of Privacy Protection, DATCP website at: http://www.privacy.wi.gov/.
4. The Federal Trade Commission's website on identity theft at: http://www.identitytheft.gov/.

Glossary

DATCP: The state Department of Agriculture, Trade and Consumer Protection.

Do-Not-Call Registry: The federal telephone nonsolicitation directory maintained by the FTC.

FTC: Federal Trade Commission.

Wisconsin Legislative Council
One East Main Street, Suite 401
Madison, WI 53703-3382
Phone: (608) 266-1304