PRIVACY OF ELECTRONIC COMMUNICATIONS

MELINDA J. CATERINE, ESQ.

FISHER & PHILLIPS LLP
400 CONGRESS STREET
PORTLAND, ME 04101
(207) 774-6001
mcaterine@laborlawyers.com

PRIVACY OF ELECTRONIC COMMUNICATIONS[1]

1. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act of 1986 ("ECPA") governs the monitoring of electronic communications in the workplace, if the communication system affects interstate commerce. Title I of the ECPA prohibits the unauthorized interception of wire, oral, or electronic communications. Title I has three general exceptions: 1) the consent exception; 2) the business extension exception; and 3) the provider exception. Title II of the ECPA prohibits unlawful access to stored electronic communications. Title II has two general exceptions: 1) the consent exception; and 2) the provider exception.

a. Title I of the ECPA

Title I of the ECPA generally prohibits the following conduct: 1) intentionally intercepting or endeavoring to intercept electronic communications; 2) intentionally using or endeavoring to use electronic communications that have been obtained through interception; or 3) intentionally disclosing or endeavoring to disclose to any other person the contents of the electronic communications that have been obtained through interception. 18 U.S.C. § 2511(1)(a). Interception is defined as, " the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data

[1] These materials are provided for educational purposes only and are not intended as legal advice or as a substitute for legal advice. Legal advice should be obtained from a qualified attorney who is familiar with all of the pertinent facts pertaining to the case.

or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, …" 18 U.S.C. § 2510(12).

i. Business Extension Exception

Under the business extension exception, the monitoring of electronic communications is not a violation of the ECPA if: 1) it is done in the ordinary course of business; and 2) certain limited types of equipment are used to monitor the communications. This exception is derived from the definition of "electronic, mechanical or other device," which means:

> any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than –
>
> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider or wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties …

18 U.S.C. § 2510(5)(a).

For the business extension exception to apply, the device that is used to intercept the communication "must be furnished to the user by the phone company or connected to the phone line." Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992). However, in construing Section 2510(5)(a), the First Circuit has concluded that the exception does not

require that the acquisition device be configured by a provider of electronic communication service. Williams v. Poulos, 11 F.3d 271, 280 (1st Cir. 1993).

A number of courts have held that in order to rely on the business extension exception, the employer must demonstrate that it had a legitimate business purpose for monitoring the electronic communications.[2] See James v. Newspaper Agency Corp., 591 F.2d 579 (10th Cir. 1979)(monitoring telephone calls of telemarketing employees found to serve a legitimate business purpose); Briggs v. American Air Filter Co., Inc., 630 F.2d 414 (5th Cir. 1980) (preserving confidentiality of trade secrets found to be a legitimate business interest); Arias v. Mutual Central Alaram Services, Inc., 183 F.R.D. 407 (S.D.N.Y. 1998) (company that provides emergency services has a legitimate business interest in recording and monitoring its calls so that it can respond promptly and accurately to emergency situations). But see Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994) (bomb threat investigation did not warrant around the clock surveillance of employee telephone conversations); Watkins v. L.M. Berry & Co., 704 F.2d 577 (11th Cir. 1983) (once employer determined that phone calls were personal in nature, there was no legitimate business reason to continue to monitor the calls); Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (attempt to catch a thief did not justify monitoring phone calls for 22 hours when they were primarily personal phone calls).

---

[2] In dicta, the First Circuit commented that the business extension exception does not "direct courts to conduct an inquiry into whether a 'legitimate business purpose' for monitoring exists at the time of the challenged aural acquisition." Williams v. Poulos, 11 F.3d at 280.

ii. Consent Exception

The ECPA includes an exception to liability where one or more of the parties to the communication have consented to the interception. The statutory exception provides as follows:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d).

Consent may be express or implied. Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990). Implied consent is inferred "from surrounding circumstances indicating that the party knowingly agreed to the surveillance." Id. At 116-17.

Simply notifying employees that electronic communications may be monitored is not enough to constitute implied consent. In Williams v. Poulos, the court found that the employee had not given his implied consent to have his telephone calls monitored where he was merely told that the employer was monitoring employee telephone calls. 11 F.3d at 281-82. The First Circuit reasoned that although the employee was aware that monitoring would take place, he was not informed of the manner in which the monitoring would be conducted, or that he himself would be subjected to the monitoring. Id. Accordingly, for there to be implied consent, an employer must, at a minimum, inform its employees: 1) of the manner in which the monitoring will be conducted; and 2) that he or she will be subjected to such monitoring.

iii. Provider Exception

The ECPA also provides an exception for the providers of wire or electronic communication services. The exception reads as follows:

> It shall not be unlawful under this chapter for an operator of a switchboard or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

18 U.S.C. § 2511(2)(a)(i). Although this exception is primarily designed for use by phone companies, it may be possible for employers to use this exception if they maintain internal communication services. See U.S. v. Mullins, 992 F.2d 1472 (9th Cir. 1993) (Airline through its computerized travel reservation system, was "provider of wire or electronic communication service" within meaning of statute); U.S. v. Christman, 375 F.Supp. 1354 (N.D.Cal. 1974) (Security officer at department store was not guilty of unlawful interception to telephone conversations when he received reports of various improprieties and recorded conversations on store's privately operated telecommunications system).

b. Title II of the ECPA

Title II of the ECPA, or the Stored Communications Act, makes it unlawful to intentionally access, obtain, alter or disclose the contents of any stored electronic communication, without proper authorization. 18 U.S.C. §§ 2701(a) and 2701(a). Title

II has two general exceptions to its prohibitions: 1) the consent exception; and 2) the provider exception.

i. Consent Exception

Stored electronic communications may be lawfully accessed when there has been consent "by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). Similarly, the contents of the stored electronic communication can be disclosed, "with the lawful consent of the originator or an addressee or intended recipient of such communication …" 18 U.S.C. § 2702(b)(3).

b. Provider Exception

In addition, Title II has a special exception for service providers. As a result, access to stored communications is permissible if it has been authorized "by the person or entity providing a wire or electronic communication service." 18 U.S.C. § 2701(c)(1). Accordingly, an employer who accesses or monitors stored electronic communications will fall within the exception if it is deemed to be the entity providing the wire or electronic communication service. In Bohach v. Reno, 932 F.Supp. 1232, 1235 (D.Nev.1996), the city was retrieving stored messages from its Alphapage system. The court found that the Reno Police Department was a "service provider" with regard to the Alphapage system and could "do as they wish when it comes to accessing communications in electronic storage."

2. E-Mail Policy

It is important to have an e-mail policy in your employee handbook so that employees will understand that the same confidentiality, anti-harassment, non-

solicitation, and other such policies apply to the use of e-mail to the same extent that they apply to other conduct in the office. Employees also need to be informed that their e-mails will be monitored. This will help to limit the number of inappropriate e-mails, reduce the potential for an invasion of privacy claim, and will support a defense of informed consent. The following is a sample electronic communications policy:

ELECTRONIC, COMMUNICATIONS AND COMPUTER EQUIPMENT AND SYSTEMS

All of The Company's electronic, communication and computer equipment, systems, software and services, including but not limited to the Company's electronic mail (e-mail), voice mail equipment and systems, and internet service (collectively, the "Electronic Systems"), are the property of the Company. All communications, data, records, files and other information created through the use of, or retained in, the Electronic Systems (collectively, the "Information") are Company property. The Company makes the Electronic Systems available to its employees solely for conducting Company business.

The Company reserves the right to monitor the operation and use of the Electronic Systems and to access, review, record and disclose all Information, without prior notice to employees. Employees, contractors, clients, and suppliers using the Company's Electronic Systems do so at their own risk with the knowledge that the Company may monitor such use and access, review, record and/or disclose any and all Information resulting from such use and without any expectation of privacy. Even information that an employee deletes from the Electronic Systems may still be retrieved and accessed by the Company. Use of the Company's Electronic Systems will be deemed consent to the Company to monitor such use, and access, review, record and/or disclose any and all Information resulting from such use.

All passwords and codes used in connection with the Electronic Systems and the Information are the property of the Company. The Company may override individual passwords and codes and require employees to disclose any passwords or codes. Employees must abide by, and not attempt to circumvent, all systems' security controls, including but not limited to the passwords of other individuals. The Company prohibits employees from accessing or attempting to access or use the e-mail or voice mail systems of a co-worker, unless authorized to do so.

All employees are expected to maintain a secure environment for the Electronic Systems and Information. Accordingly, employees are required to:

* protect the Electronic Systems, software and services from all types of abuse including misuse, misappropriation, misapplication, and vandalism.
* protect the confidentiality, integrity and accuracy of Information from unauthorized access, alteration, or destruction.
* maintain the privacy of proprietary, privileged, personal, or otherwise sensitive Information. (For example, you must exercise caution when sending confidential information via e-mail since the degree to which the information remains confidential is largely dependent upon the care and protection exercised by you and the recipient of the e-mail message.)
* use computer software and other copyrighted materials in accordance with licensing agreements, notices, contracts and applicable copyright laws.
* protect the Electronic Systems and Information from viruses and other harm by not downloading software from public bulletin boards and not installing unauthorized software of any type, including personally owned software.

The Company may provide tools and equipment for remotely accessing the Company's Electronic Systems. The use of equipment and software provided by The Company for remotely accessing The Company's Electronic Systems is limited to authorized persons and for purposes relating to Company business. The Company's Information Technology Department will only provide support for equipment and software provided by The Company. The Company will bear no responsibility if the installation or use of any necessary software causes system lockups, crashes, or complete or partial data loss. In its sole discretion, The Company can terminate remote access for any employee at any time, for any reason, with or without notice.

In keeping with the policies against sexual and other forms of unlawful harassment and discrimination, The Company prohibits any use of the Electronic Systems to make offensive, harassing, vulgar, obscene, threatening, discriminatory, or intimidating communications. In addition, employees are prohibited from creating, distributing or soliciting sexually oriented messages or images using the Electronic Systems. The Company also prohibits communications that constitute slander, defamation, or unlawful trade disparagement of employees, clients, vendors or any other person or entity.

Nothing should be said in an e-mail message that would be inappropriate, improper or unsuitable to state in a written memo. Employees should regard e-mail as another form of written communication.

The Company's policy set forth above regarding confidentiality of information applies fully to Information, data, records and files within the Company's Electronic Systems. Employees may disclose Information obtained from the Company's Electronic Systems only to authorized individuals. The provisions of the Company's policy on solicitation and distribution apply fully to all electronic and telephonic communications.

Employee Acknowledgement and Consent

I hereby state that I have thoroughly read the policy set forth above, that I have had the opportunity to ask any questions I wanted to ask about the meaning or application of this policy, and that I fully and completely understand this policy. By my signature below I agree: 1) to abide by and comply with all of the provisions of this policy; 2) that I have no expectation of privacy in the use of these systems or in the messages transmitted, received or stored therein; and 3) that the Company in its sole discretion has the right (a) to monitor my operation and use of the Electronic Systems, (b) to access and review all Information which flows through or is stored within its Electronic Systems, and (c) to override any passwords or codes which I may be using and to require me to disclose any passwords or codes which I may be are using on the Electronic Systems.

Dated:

_____

Signature

3. State Statutes Governing Electronic Communications and Surveillance

STATE	REFERENCE CITATIONS
Alabama	Ala. Code §§ 13A-11-30 to 13A-11-36, 13A-5-7 and 13A-5-12
Alaska	Alaska Stat. §§ 42.20.300 to 42.20.330, 42.20.390, 12.55.035 to 12.55.036, 12.55.135
Arizona	Ariz. Rev. Stat. §§13-702, 13-801, 13-3001, 13-3005, 13-3012 to 3013, 13-3019
Arkansas	Ark. Code Ann. §§ 5-1-102(13)(A), 5-2-501(1), 5-4-201, 5-4-401, 5-16-101, 5-60-120
California	**Coverage:** Audio/video recording: Cal. Lab. Code § 435; Cal. Penal Code §§ 630 to 637 **Audio/visual surveillance:** Cal. Lab. Code § 435; Cal. Penal Code §§ 630 to 637 Location monitoring: Cal. Lab. Code § 435; Cal. Penal Code §§ 630 to 637 Telephone monitoring: Cal. Lab. Code § 435; Cal. Penal Code §§ 630

	to 637 Microchip implantation: Cal. Civ. Code § 52.7 RFID monitoring: Calif. Chap. 746 (S.B. 31), L. 2008 **Monitoring Restrictions or Prohibitions:** Audio/video recording: Cal. Penal Code § 632 Audio/visual surveillance: Cal. Lab. Code § 435 Location monitoring: Cal. Penal Code § 637.7 Telephone monitoring: Cal. Penal Code §§ 632, 632.5, 632.6, 632.7; 1983 Cal. Regulatory Notice Reg. 107-B (July 1, 1983) Microchip implantation: Cal. Civ. Code § 52.7 RFID monitoring: Calif. Chap. 746 (S.B. 31), L. 2008 **Administration/Enforcement:** Audio/video recording: Cal. Gov't Code § 12511; Cal. Penal Code § 637.2 Audio/visual surveillance: Cal. Lab. Code § 59 Location monitoring: Cal. Gov't Code § 12511; Cal. Penal Code § 637.2 Telephone monitoring: Cal. Gov't Code § 12511; Cal. Penal Code § 637.2; Cal. Pub. Util. Code § 703 Microchip implantation: Cal. Gov't Code § 12511; Cal. Civ. Code § 52.7 RFID monitoring: Cal. Gov't Code § 12511; Calif. Chap. 746 (S.B. 31), L. 2008 **Penalties/Remedies:** Audio/video recording: Cal. Penal Code §§ 632, 637.2 Audio/visual surveillance: Cal. Lab. Code § 435; Cal. Penal Code § 19.8 Location monitoring: Cal. Penal Code §§ 19, 637.7 Telephone monitoring: Cal. Penal Code §§ 632, 637.2 Microchip implantation: Cal. Civ. Code § 52.7 RFID monitoring: Calif. Chap. 746 (S.B. 31), L. 2008
Colorado	Colo. Rev. Stat. §§ 18-1.3-401, 18-9-301 to 18-9-305
Connecticut	Conn. Gen. Stat. §§ 31-48b, 31-48d, 31-50, 52-570d, 53a-35a, 53a-41, 53a-187 to 53a-89
Delaware	Del. Code Ann. tit. 11, §§ 1335, 2401 to 2402, 4205, 4206, 4208; tit. 19, §§ 105, 705
District of Columbia	D.C. Code Ann. §§ 23-541 to 23-542, 23-556
Florida	**Monitoring Restrictions and Prohibitions:** Fla. Stat. Ann. ch. 934.02, 934.03 **Penalties/Remedies:** Fla. Stat. Ann. ch. 775.082, 775.083, 934.03, 934.10, 934.41
Georgia	Ga. Code Ann. §§ 16-11-60, 16-11-62, 16-11-64, 16-11-65, 16-11-66, 16-11-69

Hawaii	**Telephone monitoring:** Haw. Rev. Stat. §§ 803-41, 803-42, 803-48 **Audio/visual monitoring:** Haw. Rev. Stat. §§ 711-1111 **Penalties/remedies:** Haw. Rev. Stat. §§ 706-606, 706-621, 706-640, 706-660, 706-663, 803-48
Ohio	Idaho Code §§ 18-101, 18-6701, 18-6702, 18-6709, 18-6712
	Coverage: 720 Ill. Comp. Stat. Ann. 5/14-1 to 5/14-9; 720 Ill. Comp. Stat. Ann. 5/26-4 **Monitoring Restrictions or Prohibitions:** Audio/video recording: 720 Ill. Comp. Stat. Ann. 5/14-1 to 5/14-6 Audio/visual surveillance: 720 Ill. Comp. Stat. Ann. 5/26-4 Computer monitoring: 720 Ill. Comp. Stat. Ann. 5/14-1 to 5/14-2 Location monitoring: 720 Ill. Comp. Stat. Ann. 5/14-1 to 5/14-2 Telephone monitoring: 720 Ill. Comp. Stat. Ann. 5/14-1 to 5/14-6 **Administration/Enforcement:** 55 Ill. Comp. Stat. Ann. 5/3-9005; 720 Ill. Comp. Stat. Ann. 5/14-6, 5/14-8 **Penalties/Remedies:** Audio/video recording: 720 Ill. Comp. Stat. Ann. 5/14-4; 730 Ill. Comp. Stat. Ann. 5/5-8-1 Audio/visual surveillance: 720 Ill. Comp. Stat. Ann. 5/26-4; 730 Ill. Comp. Stat. Ann. 5/5-5-2, 5/5-9-1 Computer monitoring: 720 Ill. Comp. Stat. Ann. 5/14-4; 730 Ill. Comp. Stat. Ann. 5/5-8-1, 5/5-9-1 Location monitoring: 720 Ill. Comp. Stat. Ann. 5/14-4; 730 Ill. Comp. Stat. Ann. 5/5-8-1, 5/5-9-1 Telephone monitoring: 720 Ill. Comp. Stat. Ann. 5/14-4; 730 Ill. Comp. Stat. Ann. 5/5-8-1, 5/5-9-1
Indiana	Ind. Code §§ 1-1-4-5; 35-33.5-1-1, 35-33.5-5-4 to 35-33.5-5-5, 35-50-2-6
Iowa	Iowa Code §§ 727.8, 808B.1, 808B.2, 808B.8, 902.9, 903.1
Kansas	Kan. Stat. Ann. §§ 21-3110, 21-3206, 21-3207, 21-4001, 21-4002, 21-4502, 21-4503a, 21-4607, 22a-104, 44-618, 44-808, 75-5701
Kentucky	Ky. Rev. Stat. Ann. §§ 15.210, 69.013, 500.080(12), 526.010, 526.020, 526.070, 532.060, 534.030, 534.050
Louisiana	La. Rev. Stat. Ann. §§ 15-1302 to 15-1303, 15-1312, 16-1
Maine	15 M.R.S.A. § 709 et seq.
Maryland	Md. Code Ann. Ct. & Jud. Proc. §§ 10-401, 10-402, 10-410 Md. Code Ann. State Gov't § 9-1205
Massachusetts	Mass. Gen. Laws ch. 272, § 99
Michigan	Mich. Comp. Laws §§ 750.539a, 750.539c, 750.539g, 750.539h
Minnesota	Minn. Stat. §§ 175.121, 179.12, 626A.01, 626A.02, 626A.13
Mississippi	Miss. Code Ann. §§ 19-23-11, 41-29-501, 41-29-503, 41-29-529 to 41-29-533

Missouri	**Coverage:** Telephone monitoring: Mo. Rev. Stat. § 542.400 Microchip implantation: Mo. 285.035 (H.B. 1883), L. 2008 Restrictions or Prohibitions: Telephone monitoring: Mo. Rev. Stat. § 542.402 Microchip implantation: Mo. 285.035 (H.B. 1883), L. 2008 **Notification Requirements:** Mo. Rev. Stat. § 542.402 **Administration/Enforcement:** Mo. Rev. Stat. § 56.060 **Penalties/Remedies:** Telephone monitoring: Mo. Rev. Stat. §§ 542.402, 558.011, 560.011 Microchip implantation: Mo. 285.035 (H.B. 1883), L. 2008
Montana	Mont. Code Ann. §§ 7-4-2712, 45-2-101(56), 45-8-213
Nebraska	Neb. Rev. Stat. §§ 6-271 to 6-290, 28-105, 28-109, 86-295, 86-297, 884-203 to 884-204
Nevada	Nev. Rev. Stat. §§ 193.0205, 193.130(2)(d), 252.080, 200.610, 200.620, 200.650, 200.690
New Hampshire	N.H. Rev. Stat. Ann. §§ 570-A:1, 570-A:2, 570-A:11, 651:2, 625:9(IV)
New Jersey	N.J. Stat. Ann. §§ 2A:156A-1 to 2A:156A-5, 2A:156A-17, 2A:156A-24, 2A:156A-25, 2A:156A-28, 2A:158-4, 2C:43-3, 2C:43-6
New Mexico	N.M. Stat. Ann. §§ 30-1-12(E), 30-12-1, 30-12-9, 30-12-11, 31-19-1, 36-1-18
New York	**Coverage:** N.Y. Penal Law § 250.00; N.Y. Lab. Law §§ 203-c, 701 **Monitoring Restrictions or Prohibitions:** Audio/visual surveillance: N.Y. Lab. Law § 203-c Telephone monitoring: N.Y. Penal Law §§ 250.00, 250.05 Union-related activities monitoring: N.Y. Lab. Law §§ 701, 704 Retaliation Prohibition: N.Y. Lab. Law § 215 **Administration/Enforcement:** Audio/visual surveillance: N.Y. Lab. Law §§ 203-c, 215 Telephone monitoring: N.Y. Exec. Law § 63; N.Y. Lab. Law § 214 Retaliation Prohibition: N.Y. Lab. Law § 215 Union-related activities monitoring: N.Y. Lab. Law § 706 **Penalties/Remedies:** Audio/visual surveillance: N.Y. Lab. Law § 203-c Retaliation Prohibition: N.Y. Lab. Law § 215 Telephone monitoring: N.Y. Crim. Pro. Law §§ 700.05 to 700.10; N.Y. Penal Law §§ 70.00, 80.00, 80.10, 250.05 Union-related activities monitoring: N.Y. Lab. Law §§ 701, 704
North Carolina	N.C. Gen. Stat. §§ 15A-286 to 15A-287, 15A-296
North Dakota	**Coverage:** Telephone/computer monitoring: N.D. Cent. Code § 12.1-15-02

	Microchip implantation: N.D. Cent. Code § 12.1-15-06 **Monitoring Restrictions and Prohibitions:** Telephone/computer monitoring: N.D. Cent. Code §§ 12.1-01-04, 12.1-15-02, 12.1-15-04 Microchip implantation: N.D. Cent. Code § 12.1-15-06 **Notification Requirements:** Telephone/computer monitoring: N.D. Cent. Code §§ 12.1-01-04, 12.1-15-02, 12.1-15-04 **Administration/Enforcement:** Telephone/computer monitoring: N.D. Cent. Code § 11-16-01 Microchip implantation: N.D. Cent. Code § 11-16-01 **Penalties/Remedies:** Telephone/computer monitoring: N.D. Cent. Code §§ 12.1-03-02, 12.1-03-03, 12.1-03-04, 12.1-15-02, 12.1-32-01, 12.1-32—01.1, 12.1-32-02, 12-32-03 Microchip implantation: N.D. Cent. Code §§ 12.1-03-02, 12.1-03-03, 12.1-03-04, 12.1-15-06, 12.1-32-01, 12.1-32-01.1, 12-32-03
Ohio	Ohio Rev. Code Ann. §§ 2929.14, 2929.18, 2933.51, 2933.52, 2933.65
Oklahoma	E-mail/telephone monitoring: Okla. Stat. tit. 13, §§ 176.1 to 176.6 Microchip implantation: Okla. S.B. 47, L. 2008
Oregon	**Coverage:** Or. Rev. Stat. §§ 133.721, 163.700, 165.535, 165.540, 165.543 **Monitoring Restrictions or Prohibitions:** Audio/video recording: Or. Rev. Stat. §§ 133.721, 165.535, 165.540 Audio/visual surveillance: Or. Rev. Stat. § 163.700 Telephone monitoring: Or. Rev. Stat. §§ 133.721, 165.535, 165.540 **Administration/Enforcement:** Or. Rev. Stat. §§ 8.650, 133.739 **Penalties/Remedies:** Or. Rev. Stat. §§ 133.739, 161.615, 161.635, 161.655, 161.665, 163.700, 165.543
Pennsylvania	18 Pa. Cons. Stat. §§ 1101, 1103, 5702 to 5704, 5725, 5728
Puerto Rico	No State-Mandated Notice or Consent Requirements for Telephone Monitoring
Rhode Island	R.I. Gen. Laws §§ 11-35-21, 12-5.1-1, 28-6.12-1
South Carolina	S.C. Code Ann. §§ 17-30-10 to 17-30-20, 17-30-30, 17-30-40, 17-30-50, 17-30-65, 17-30-135
South Dakota	**Coverage:** S.D. Codified Laws 23A-35A-1, 23A-35A-20 **Monitoring Restrictions or Prohibitions:** Audio/video recording: S.D. Codified Laws §§ 23A-35A-1, 23A-35A-20 Telephone monitoring: S.D. Codified Laws §§ 23A-35A-1, 23A-35A-20 **Administration/Enforcement:** S.D. Codified Laws § 7-16-9 **Penalties/Remedies:** S.D. Codified Laws § 22-6-1

Tennessee	Tenn. Code Ann. §§ 39-13-601 to 39-13-604, 40-35-111
Texas	Tex. Penal Code Ann. §§ 12.33, 16.02 Tex. Crim. Proc. Code Ann. § 18.20
Utah	Utah Code Ann. §§ 76-1-601, 76-3-203 to 76-3-204, 76-3-301 to 76-3-302, 76-9-401 to 76-9-403, 76-9-406
Vermont	No State-Mandated Notice or Consent Requirements for Telephone Monitoring
Virginia	Va. Code Ann. §§ 18.2-10 to 18.2-11, 18.2-167, 19.2-61 to 19.2-62, 19.2-69
Washington	Wash. Rev. Code §§ 9.73.030, 9.73.060, 9.73.070, 9.73.080, 9A.20.021(2), 36.27.020
West Virginia	W. Va. Code §§ 61-3-24c, 62-1D-2, 62-1D-3, 62-1D-6, 62-1D-12
Wisconsin	**Coverage:** Telephone/computer monitoring: Wis. Stat. § 968.31 Labor relations: Wis. Stat. § 111.06 Microchip implantation: Wis. Stat. § 146.25 **Monitoring Restrictions and Prohibitions:** Telephone/computer monitoring: Wis. Stat. §§ 968.27, 968.31 Labor relations: Wis. Stat. § 111.06 Microchip implantation: Wis. Stat. § 146.25 **Notification Requirements:** Telephone/computer monitoring: Wis. Stat. § 968.31 **Administration/Enforcement:** Telephone/computer monitoring: Wis. Stat. §§ 968.31, 978.05 Labor relations: Wis. Stat. §§ 111.02, 111.07 Microchip implantation: Wis. Stat. § 978.05 **Penalties/Remedies:** Telephone/computer monitoring: Wis. Stat. §§ 968.31, 939.50 Labor relations: Wis. Stat. § 111.07 Microchip implantation: Wis. Stat. § 146.25
Wyoming	Wyo. Stat. Ann. §§ 7-3-702, 7-3-710, 8-1-102