Growing risks and legal implications exist when employers ask applicants and employees for their passwords to social media sites. A number of states have enacted legislation to prohibit employers from requiring access to social media passwords. A federal bill has also been introduced to prohibit the practice. The Social Networking Online Protection Act (SNOPA) would prohibit employers from requiring current employees or applicants to provide a username, password or other access to online content. The bill would bar employers from disciplining employees who refuse to volunteer such information.

If a state does not appear on the following chart, it is because we have not found a state statute on the topic.

To check whether there is pending or recently enacted legislation, please click here.

To access additional SHRM State Law & Regulation Resources click here.

Please note: This material is for personal use only and is protected by U.S. Copyright Law (Title 17 USC). It is provided as general information only and does not constitute and is not a substitute for legal or other professional advice. Reliance upon this material is solely at your own risk.

<table>
<thead>
<tr>
<th>State</th>
<th>Statute</th>
</tr>
</thead>
</table>
| Arkansas | 11-2-124. Social media accounts of current and prospective employees. (a) As used in this section: (1) "Employee" means an individual who provides services or 30 labor for wages or other remuneration for an employer; (2) "Employer" means a person or entity engaged in business, an industry, a profession, a trade, or other enterprise in the state or a unit of state or local government, including without limitation an agent, representative, or designee of the employer; and (3)(A) "Social media account" means a personal account with an electronic medium or service where users may create, share, or view user-generated content, including without limitation: (i) Videos; (ii) Photographs; (iii) Blogs; (iv) Podcasts; (v) Messages; (vi) Emails; or (vii) Website profiles or locations. (B) "Social media account" does not include an account: (i) Opened by an employee at the request of an employer; (ii) Provided to an employee by an employer such as a company email account or other software program owned or operated exclusively by an employer; (iii) Setup by an employee on behalf of an employer; (iv) Setup by an employee to impersonate an employer through the use of the employer's name, logos, or trademarks. (C) "Social media account" includes without limitation an account established with Facebook, Twitter, LinkedIn, MySpace, or Instagram. (b)(1) An employer shall not require, request, suggest, or cause a current or prospective employee to: (A) Disclose his or her username and password to the current or prospective employee's social media account; (B) Add an employee, supervisor, or administrator to the list or 24 contacts associated with his or her social media account; or (C) Change the privacy settings associated with his or her social media account. (2) If an employer inadvertently receives an employee's username, password, or other login information to the employee's social media account through the use of an electronic device provided to the employee by the employer or a program that monitors an employer's network the employer is not liable for having the information but may not use the information to gain access to an employee's social media account. (c) An employer shall not: (1) Take action against or threaten to discharge, discipline, or otherwise penalize a current employee for exercising his or her rights under subsection (b) of this section; or (2) Fail or refuse to hire a prospective employee for exercising his or her rights under subsection (b) of this section. (d) This section does not prohibit an employer from viewing information about a current or prospective employee that is publicly available on the Internet. (e) Nothing in this section: (1) Prevents an employer from complying with the requirements of federal, state, or local laws, rules, or regulations or the rules or regulations of self-regulatory organizations; or (2)(A) Affects an employee's existing rights or obligations to request an employee to disclose his or her username and password for the purpose of accessing a social media account if the employee's
California

980. (a) As used in this chapter: (1) "Employer" means a private employer or a public employer. (2) "Social media" means an electronic service or account, or electronic content, including, but not limited to, videos, still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations. (b) An employer shall not require or request an employer or applicant for employment to do any of the following: (1) Disclose a username or password for the purpose of accessing personal social media. (2) Access personal social media in the presence of the employer. (3) Divulge any personal social media, except as provided in subdivision (c). (c) Nothing in this section shall affect an employer's existing rights and obligations to request an employee to divulge personal social media reasonably believed to be relevant to an investigation of allegations of employee misconduct or employee violation of applicable laws and regulations, provided that the social media is used solely for purposes of that investigation or a related proceeding. (d) Nothing in this section precludes an employer from requiring or requesting an employee to disclose a username, password, or other method for the purpose of accessing an employer-issued electronic device. (e) An employer shall not discharge, discipline, threaten to discharge or discipline, or otherwise retaliate against an employee or applicant for not complying with a request or demand by the employer that violates this section. However, this section does not prohibit an employer from terminating or otherwise taking an adverse action against an employee or applicant if otherwise permitted by law. SEC. 2. Because of the crucial privacy rights at issue and the growing abuse of those rights, the Legislature finds and declares that this act addresses a matter of statewide interest and applies to public employers generally, including charter cities and counties.

99120. As used in this chapter, "social media" means an electronic service or account, or electronic content, including, but not limited to, videos or still photographs, blogs, video blogs, podcasts, instant and text messages, email, online services or accounts, or Internet Web site profiles or locations.

99121. (a) Public and private postsecondary educational institutions, and their employees and representatives, shall not require or request a student, prospective student, or student group to do any of the following: (1) Disclose a user name or password for accessing personal social media. (2) Access personal social media in the presence of the institution's employee or representative. (3) Divulge any personal social media information. (b) A public or private postsecondary educational institution, or its representative, shall not:

- Disclose a user name or password for accessing personal social media.
- Require or request an employee or student or a student group or any other representative to disclose a user name or password or any other personal social media account activity.
- Require or request a student, prospective student, or student group to disclose a user name or password or any other personal social media account activity.
institutions shall not suspend, expel, discipline, threaten to take any of those actions, or otherwise penalize a student, prospective student, or student group in any way for refusing to comply with a request or demand that violates this section. (c) This section shall not do either of the following: (1) Affect a public or private postsecondary educational institution's existing rights and obligations to protect against and investigate alleged student misconduct or violations of applicable laws and regulations. (2) Prohibit a public or private postsecondary educational institution from taking any adverse action against a student, prospective student, or student group for any lawful reason.

**Colorado 8-2-126. Prohibitions of employer - requiring access to personal electronic communication devices - definitions.** (1) AS USED IN THIS SECTION: (a) "APPLICANT" MEANS AN APPLICANT FOR EMPLOYMENT. (b) "ELECTRONIC COMMUNICATIONS DEVICE" MEANS A DEVICE THAT USES ELECTRONIC SIGNALS TO CREATE, TRANSMIT, AND RECEIVE INFORMATION, INCLUDING COMPUTERS, TELEPHONES, PERSONAL DIGITAL ASSISTANTS, AND OTHER SIMILAR DEVICES. (c) "EMPLOYER" MEANS A PERSON ENGAGED IN A BUSINESS, INDUSTRY, PROFESSION, TRADE, OR OTHER ENTERPRISE IN THE STATE OR A UNIT OF STATE OR LOCAL GOVERNMENT. "EMPLOYER" INCLUDES AN AGENT, A REPRESENTATIVE, OR A DESIGNEE OF THE EMPLOYER. (2) (a) AN EMPLOYER MAY NOT REQUEST OR REQUIRE THAT AN EMPLOYEE OR APPLICANT DISCLOSE ANY USER NAME, PASSWORD, OR OTHER MEANS FOR ACCESSING THE EMPLOYEE'S OR APPLICANT'S PERSONAL ACCOUNT OR SERVICE THROUGH THE EMPLOYEE'S OR APPLICANT'S ELECTRONIC COMMUNICATIONS DEVICE. (b) PARAGRAPH (a) OF THIS SUBSECTION (2) DOES NOT PROHIBIT AN EMPLOYER FROM REQUESTING AN EMPLOYEE TO DISCLOSE ANY USER NAME, PASSWORD, OR OTHER MEANS FOR ACCESSING NONPERSONAL ACCOUNTS OR SERVICES THAT PROVIDE ACCESS TO THE EMPLOYER'S INTERNAL COMPUTER OR INFORMATION SYSTEMS. (3) AN EMPLOYER SHALL NOT: (a) DISCHARGE, DISCIPLINE, OR OTHERWISE PENALIZE OR THREATEN TO DISCHARGE, DISCIPLINE, OR OTHERWISE PENALIZE AN EMPLOYEE FOR AN EMPLOYEE'S REFUSAL TO DISCLOSE ANY INFORMATION SPECIFIED IN PARAGRAPH (a) OF SUBSECTION (2) OF THIS SECTION; OR (b) FAIL OR REFUSE TO HIRE AN APPLICANT BECAUSE THE APPLICANT REFUSES TO DISCLOSE ANY INFORMATION SPECIFIED IN PARAGRAPH (a) OF SUBSECTION (2) OF THIS SECTION. (4) THIS SECTION DOES NOT PREVENT AN EMPLOYER FROM: (a) CONDUCTING AN INVESTIGATION TO ENSURE COMPLIANCE WITH APPLICABLE SECURITIES OR FINANCIAL LAW OR REGULATORY REQUIREMENTS BASED ON THE RECEIPT OF INFORMATION ABOUT THE USE OF A PERSONAL WEB SITE, INTERNET WEB SITE, WEB-BASED ACCOUNT, OR SIMILAR ACCOUNT BY AN EMPLOYEE FOR BUSINESS PURPOSES; OR (b) INVESTIGATING AN EMPLOYEE'S ELECTRONIC COMMUNICATIONS BASED ON THE RECEIPT OF INFORMATION ABOUT THE UNAUTHORIZED DOWNLOADING OF AN EMPLOYEE'S PROPRIETARY INFORMATION OR FINANCIAL DATA TO A PERSONAL WEB SITE, INTERNET WEB SITE, WEB-BASED ACCOUNT, OR SIMILAR ACCOUNT BY AN EMPLOYEE. (5) AN AGGRIEVED APPLICANT OR EMPLOYEE MAY INSTITUTE A CIVIL ACTION FOR A VIOLATION OF THIS SECTION IN A COURT OF COMPETENT JURISDICTION WITHIN ONE YEAR AFTER THE DATE OF THE ALLEGED VIOLATION. IN RESPONSE TO THE ACTION, THE COURT MAY AWARD THE AGGRIEVED PERSON: (a) INJUNCTIVE RELIEF; (b) COMPENSATORY AND CONSEQUENTIAL DAMAGES INCURRED BY THE PERSON AS A RESULT OF THE VIOLATION; AND (c) REASONABLE ATTORNEY FEES AND COURT COSTS. **SECTION 2.** Safety clause. The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

**Delaware 9401. Short title.** This enactment may be known and cited as the “Education Privacy Act.”

**9402. Definitions.** (1) “Academic institution” means public or nonpublic institution of higher education or institution of postsecondary education. (2) “Applicant” means a prospective student applying for admission into the subject academic institution. (3) “Electronic communication device” means a cell telephone, personal digital assistant, electronic device with mobile data access, laptop computer, pager, broadband personal communication device whether mobile or desktop, 2-way messaging device, electronic game, or portable computing device. (4) “Social networking site” means an internet-based, personalized, privacy-protected website or application whether free or commercial that allows users to construct a private or semi-private profile site within a bounded system, create a list of other system users who are granted reciprocal access to the individual’s profile site, send and receive email, and share personal content, communications, and contacts. (5) “Student” means a person which at all relevant times is admitted into the academic institution.

**9403. Academic institution; prohibited acts.** (a) An academic institution shall not request or require that a student or applicant disclose any password or other related account information in order to gain access to the student’s or applicant’s social networking site profile or account by way of an electronic
Illinois 55/10 Sec. 10. Prohibited inquiries. (a) It shall be unlawful for any employer to inquire, in a written application or in any other manner, of any prospective employee or of the prospective employee's previous employers, whether that prospective employee has ever filed a claim for benefits under the Workers' Compensation Act or Workers' Occupational Diseases Act or received benefits under these Acts. (b)(1) Except as provided in this subsection, it shall be unlawful for any employer to request or require any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website or to demand access in any manner to the employee's or prospective employee's account or profile on a social networking website. (2) Nothing in this subsection shall limit an employer's right to: (A) promulgate and maintain lawful workplace policies governing the use of the employer's electronic equipment, including policies regarding Internet use, social networking site use, and electronic mail use; and (B) monitor usage of the employer's electronic equipment and the employer's electronic mail without requesting or requiring any employee or prospective employee to provide any password or other related account information in order to gain access to the employee's or prospective employee's account or profile on a social networking website. (3) Nothing in this subsection shall prohibit an employer from obtaining about a prospective employee or an employee information that is in the public domain or that is otherwise obtained in compliance with this amendatory Act of the 97th General Assembly. (3.5) Provided that the password, account information, or access sought by the employer relates to a professional account, and not a personal account, nothing in this subsection shall prohibit or restrict an employer from complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications as required under Illinois insurance laws or federal law or by a self-regulatory organization as defined in Section 3(A)(26) of the Securities Exchange Act of 1934, 15 U.S.C. 78(A)(26). (4) For the purposes of this subsection, "social networking website" means an Internet-based service that allows individuals to: (A) construct a public or semi-public profile within a bounded system, created by the service; (B) create a list of other users with whom they share a connection within the system; and (C) view and navigate their list of connections and those made by others within the system. "Social networking website" shall not include electronic mail. For the purposes of paragraph (3.5) of this subsection, "professional account" means an account, service, or profile created, maintained, used, or accessed by a current or prospective employee for business purposes of the employer. For the purposes of paragraph (3.5) of this subsection, "personal account" means an account, service, or profile on a social networking website that is used by a current or prospective employee exclusively for personal communications unrelated to any business purposes of the employer.

Public Act 098-0129 AN ACT concerning education. Be it enacted by the People of the State of Illinois, represented in the General Assembly: Section 1. Short title. This Act may be cited as the Right to Privacy in the School Setting Act. Section 5. Definitions. In this Act: "Elementary or secondary school" means a public elementary or secondary school or school district or a nonpublic school recognized by the State Board of Education. "Post-secondary school" means an institution of higher learning as defined in the Higher Education Student Assistance Act. "Social networking website" means an Internet-based service that allows individuals to do the following: (1) construct a public or semi-public profile within a bounded system created by the service; (2) create a list of other users with whom they share a connection within the system; and (3) view and navigate their list of connections and those made by others within the system. "Social networking website" does not include electronic mail. Section 10. Prohibited inquiry. (a) It is unlawful for a post-secondary school to request or require a student or his or her parent or guardian to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website or to demand access in any manner to a student's account or profile on a social networking website. (b) Nothing in this Section limits a post-secondary school's right to do the following: (1) promulgate and maintain lawful school policies governing the use of the post-secondary school's electronic equipment, including policies regarding Internet use, social networking website use, and electronic mail use; and (2) monitor usage of the post-secondary school's electronic equipment and the post-secondary school's electronic mail without requesting or requiring a student to provide a password or other related account information in order to gain access to the student's account or profile on a social networking website. (c) Nothing in this Section prohibits a post-secondary school from obtaining information about a student that is in the public domain or that is otherwise obtained in compliance with this Act. (d) This Section does not apply when a post-secondary school has reasonable cause to believe that a student's account on a social networking website contains evidence that the student has violated a school disciplinary rule or policy. Section 15. Notification. An elementary or secondary school must provide notification to the student and his or her parent or guardian that the elementary or secondary school may request or require a student to provide a password or other related account information in order to gain access to the student's account or
### New Jersey

**P.L.2012, CHAPTER 75** AN ACT prohibiting the requirement to disclose personal information for certain electronic communications devices by institutions of higher education. **BE IT ENACTED by the Senate and General Assembly of the State of New Jersey:** 1. For purposes of this act: “Applicant” means an applicant for admission into a public or private institution of higher education. “Electronic communications device” means any device that uses electronic signals to create, transmit, and receive information, including a computer, telephone, personal digital assistant, or other similar device. “Public or private institution of higher education” means any public or private institution of higher education or any employee, agent, representative, or designee of the institution. “Social networking website” means an Internet-based service that allows individuals to construct a public or semi-public profile within a bounded system created by the service, create a list of other users with whom they share a connection within the system, and view and navigate their list of connections and those made by others within the system. 2. No public or private institution of higher education in this State shall: a. Require a student or applicant to provide or disclose any user name or password, or in any way provide access to, a personal account or service through an electronic communications device. b. In any way inquire as to whether a student or applicant has an account or profile on a social networking website. c. Prohibit a student or applicant from participating in activities sanctioned by the institution of higher education, or in any other way discriminate or retaliate against a student or applicant, as a result of the student or applicant refusing to provide or disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device as provided in subsection a. of this section. 3. No public or private institution of higher education in this State shall require a student or applicant to waive or limit any protection granted under this act. An agreement to waive any right or protection under this act is against the public policy of this State and is void and unenforceable. Upon violation of any provision of this act, an aggrieved person may, in addition to any other available remedy, institute a civil action in a court of competent jurisdiction, within one year from the date of the alleged violation. In response to the action, the court may, as it deems appropriate, order or award any one or more of the following: a. With respect to an applicant: (1) injunctive relief; (2) compensatory and consequential damages incurred by the applicant as a result of the violation, taking into consideration any failure to admit the applicant in connection with the violation; and (3) reasonable attorneys’ fees and court costs. b. With respect to a current or former student: (1) injunctive relief as it deems appropriate; (2) compensatory and consequential damages incurred by the student or former student as a result of the violation; and (3) reasonable attorneys’ fees and court costs. This act shall take effect immediately. This bill prohibits a public or private institution of higher education in this State from requiring a student or applicant to provide or disclose any user name or password, or in any way provide access to, a personal account or service through an electronic communications device. The bill also prohibits a public or private institution of higher education from prohibiting a student or applicant from participating in activities sanctioned by the institution of higher education, or in any other way discriminating or retaliating against a student or applicant, as a result of the student or applicant refusing to provide or disclose any user name, password, or other means for accessing a personal account or service through an electronic communications device. The bill prohibits a public or private institution of higher education from requiring a student or applicant to waive or limit any protection granted under the bill. Also, any current or former student or applicant aggrieved under the provisions of the bill may bring action in a court of competent jurisdiction for appropriate injunctive relief and damages, including reasonable attorneys’ fees and court costs. Finally, for purposes of the bill: “applicant” means an applicant for admission into a public or private institution of higher education; “electronic communications device” means any device that uses electronic signals to create, transmit, and receive information, including a computer, telephone, personal digital assistant, or other similar device; “public or private institution of higher education” means any public or private institution of higher education or any employee, agent, representative, or designee of the institution; and “social networking website” means an Internet-based service that allows individuals to construct a public or semipublic profile within a bounded system created by the service, create a list of other users with whom they share a connection within the system, and view and navigate their list of connections and those made by others within the system. Prohibits requirement to disclose user name, password, or other means for accessing account or service through electronic communications devices by institutions of higher education.

### Nevada

Chapter 613 Sec. 1.1. As used in sections 1.1 to 1.9, inclusive, of this act, unless the context otherwise requires, the words and terms defined in sections 1.2 to 1.5, inclusive, of this act have the meanings ascribed to them in those sections. Sec. 1.2. “Consumer credit report” means any written, oral or other communication of information by a consumer reporting agency bearing on the credit worthiness, credit standing or credit capacity of a person. Sec. 1.3. “Consumer reporting agency” has the meaning ascribed to it in NRS 686A.640. Sec. 1.4. “Credit information” means any information that is related to credit and derived from a consumer credit report or found on a consumer credit report. The term does not include information that is not related to credit, regardless of whether it is contained in a
“Employer” has the meaning ascribed to it in subsection 1 of NRS 613.440. Sec. 1.6. Except as otherwise provided in section 1.7 of this act, it is unlawful for any employer in this State to: 1. Directly or indirectly, require, request, suggest or cause any employee or prospective employee to submit a consumer credit report or other credit information as a condition of employment; 2. Use, accept, refer to or inquire concerning a consumer credit report or other credit information; 3. Discharge, discipline, discriminate against in any manner or deny employment or promotion to, or threaten to take any such action against any employee or prospective employee: (a) Who refuses, declines or fails to submit a consumer credit report or other credit information; or (b) On the basis of the results of a consumer credit report or other credit information; or 4. Discharge, discipline, discriminate against in any manner or deny employment or promotion to, or threaten to take any such action against, any employee or prospective employee who has: (a) Filed any complaint or instituted or caused to be instituted any legal proceeding pursuant to sections 1.1 to 1.9, inclusive, of this act; (b) Testified or may testify in any legal proceeding instituted pursuant to sections 1.1 to 1.9, inclusive, of this act; or (c) Exercised his or her rights, or has exercised on behalf of another person the rights afforded to him or her pursuant to sections 1.1 to 1.9, inclusive, of this act. Sec. 1.7. An employer may request or consider a consumer credit report or other credit information for the purpose of evaluating an employee or prospective employee for employment, promotion, reassignment or retention as an employee if: 1. The employer is required or authorized, pursuant to state or federal law, to use a consumer credit report or other credit information for that purpose; 2. The employer reasonably believes that the employee or prospective employee has engaged in specific activity which may constitute a violation of state or federal law; or 3. The information contained in the consumer credit report or other credit information is reasonably related to the position for which the employee or prospective employee is being evaluated for employment, promotion, reassignment or retention as an employee. The information in the consumer credit report or other credit information shall be deemed reasonably related to such an evaluation if the duties of the position involve: (a) The care, custody and handling of, or responsibility for, money, financial accounts, corporate credit or debit cards, or other assets; (b) Access to trade secrets or other proprietary or confidential information; (c) Managerial or supervisory responsibility; (d) The direct exercise of law enforcement authority as an employee of a state or local law enforcement agency; (e) The care, custody and handling of, or responsibility for, the personal information of another person; (f) Access to the personal financial information of another person; (g) Employment with a financial institution that is chartered under state or federal law, including a subsidiary or affiliate of such a financial institution; or (h) Employment with a licensed gaming establishment, as defined in NRS 463.0169. Sec. 1.8. 1. An employer who violates the provisions of sections 1.1 to 1.9, inclusive, of this act is liable to the employee or prospective employee affected by the violation. The employer is liable for any legal or equitable relief as may be appropriate, including employment of a prospective employee, reinstatement or promotion of an employee and the payment of lost wages and benefits. 2. An action to recover the liability pursuant to subsection 1 may be maintained against the employer by an employee or prospective employee: (a) For or on behalf of the employee or prospective employee; And (b) On behalf of other employees or prospective employees similarly situated. An action must not be commenced pursuant to this section more than 3 years after the date of the alleged violation. 3. In any action brought pursuant to this section, the court, in its discretion, may allow the prevailing party reasonable costs, including attorney’s fees. Sec. 1.9. 1. If any person violates sections 1.1 to 1.9, inclusive, of this act, the Labor Commissioner may impose against the person an administrative penalty of not more than $9,000 for each such violation. 2. In determining the amount of any administrative penalty to be imposed against the person, the Labor Commissioner shall consider the previous record of the person in terms of compliance with sections 1.1 to 1.9, inclusive, of this act and the severity of the violation. Any administrative penalty imposed against the person is in addition to any other remedy or penalty provided pursuant to this act. 3. The Labor Commissioner may bring a civil action pursuant to this section to restrain violations of sections 1.1 to 1.9, inclusive, of this act. A court of competent jurisdiction may issue, without bond, a temporary or permanent restraining order or injunction to require compliance with sections 1.1 to 1.9, inclusive, of this act, including any legal or equitable relief incident thereto as may be appropriate, such as employment of a prospective employee, reinstatement or promotion of an employee, and the payment of lost wages and benefits. Sec. 2. 1. It is unlawful for any employer in this State to: (a) Directly or indirectly, require, request, suggest or cause any employee or prospective employee to disclose the user name, password or any other information that provides access to his or her personal social media account. (b) Discharge, discipline, discriminate against in any manner or deny employment or promotion to, or threaten to take any such action against any employee or prospective employee who refuses, declines or fails to disclose the user name, password or any other information that provides access to his or her personal social media account. 2. It is not unlawful for an employer in this State to require an employee to disclose the user name, password or any other information to an account or a service, other than a personal social media account, for the purpose of accessing the employer’s own internal computer or information system. 3. Nothing in this
Oregon

ORS chapter 659A. SECTION 2. It is an unlawful employment practice for an employer to: (a) Require or request an employee or an applicant for employment to disclose or to provide access through the employee's or applicant's user name and password, password or other means of authentication that provides access to a personal social media account; (b) Compel an employee or applicant for employment to add the employer or an employment agency to the employee's or applicant's list of contacts associated with a social media website; (c) Except as provided in subsection (4)(b) of this section, compel an employee or applicant for employment to access a personal social media account in the presence of the employer and in a manner that enables the employer to view the contents of the personal social media account that are visible only when the personal social media account is accessed by the account holder's user name and password, password or other means of authentication; (d) Take, or threaten to take, any action to discharge, discipline or otherwise penalize an employee for the employee's refusal to disclose, or to provide access through, the employee's user name and password, password or other means of authentication that is associated with a personal social media account; (e) Require or request an employee or an applicant for employment to disclose or to provide access through the employee's or applicant's list of contacts associated with a social media website or to access a personal social media account as described in paragraph (c) of this subsection; or (f) Fail or refuse to hire an applicant for employment because the applicant refused to disclose, or to provide access through, the applicant's user name and password, password or other means of authentication that is associated with a personal social media account, to add the employer to the applicant's list of contacts associated with a social media website or to access a personal social media account as described in paragraph (c) of this subsection. (2) An employer may require an employee to disclose any user name and password, password or other means for accessing an account provided by, or on behalf of, the employer or to be used on behalf of the employer. (3) An employer may not be held liable for the failure to request or require an employee or applicant to disclose the information specified in subsection (1)(a) of this section. (4) Nothing in this section prevents an employer from: (a) Conducting an investigation, without requiring an employee to provide...
a user name and password, password or other means of authentication that provides access to a personal social media account of the employee, for the purpose of ensuring compliance with applicable laws, regulatory requirements or prohibitions against work-related employee misconduct based on receipt by the employer of specific information about activity of the employee on a personal online account or service. (b) Conducting an investigation permitted under this subsection that requires an employee, without providing a user name and password, password or other means of authentication that provides access to a personal social media account of the employee, to share content that has been reported to the employer that is necessary for the employer to make a factual determination about the matter. (c) Complying with state and federal laws, rules and regulations and the rules of self-regulatory organizations. (5) Nothing in this section prohibits an employer from accessing information available to the public about the employee or applicant that is accessible through an online account. (6) If an employer inadvertently receives the user name and password, password or other means of authentication that provides access to a personal social media account of an employee through the use of an electronic device or program that monitors usage of the employer's network or employer-provided devices, the employer is not liable for having the information but may not use the information to access the personal social media account of the employee. (7) As used in this section, 'social media' means an electronic medium that allows users to create, share and view user-generated content, including, but not limited to, uploading or downloading videos, still photographs, blogs, video blogs, podcasts, instant messages, electronic mail or Internet website profiles or locations.

SECTION 1. A public or private educational institution may not: (a) Require, request or otherwise compel a student or prospective student to disclose or to provide access to a personal social media account through the student's or prospective student's user name and password, password or other means of authentication that provides access. (b) Require, request or otherwise compel a student or prospective student to access a personal social media account in the presence of an administrator or other employee of the educational institution in a manner that enables the administrator or employee to observe the contents of the personal social media account. (c) Take, or threaten to take, any action to discipline or to prohibit from participation in curricular or extracurricular activities a student or prospective student for refusal to disclose the information or take actions specified in paragraph (a) or (b) of this subsection. (d) Fail or refuse to admit a prospective student as a result of the refusal by the prospective student to disclose the information or take actions specified in paragraph (a) or (b) of this subsection. (2) Nothing in this section prohibits an educational institution from: (a) Conducting an investigation, for the purpose of ensuring compliance with applicable law, regulatory requirements or prohibitions against student misconduct, that is based on the receipt of specific information about activity associated with a personal social media account. (b) Conducting an investigation authorized under paragraph (a) of this subsection that requires the student to share specific content on a social media account with the educational institution in order for the educational institution to make a factual determination about that content. Student cooperation required under this paragraph does not include providing the student's user name and password, password or other means of authentication that provides access to the student's personal social media account to the educational institution. (c) Revoking a student's access, in whole or in part, to equipment or computer networks owned or operated by the educational institution. (3) An educational institution is not liable for obtaining the user name and password, password or other means of authentication that provides access to a student's social media account through the application of the educational institution's policies governing the use of university equipment or computer networks owned or operated by the educational institution. However, the educational institution may not use the information obtained without the voluntary consent of the student. (4) Nothing in this section applies to social media accounts intended for use solely for educational purposes at an educational institution or to social media accounts that are created by the educational institution and provided to the student if the student has been provided advance notice that the account may be monitored at any time by the educational institution. (5) As used in this section: (a) 'Educational institution' means an institution that offers participants, students or trainees an organized course of study or training that is academic, technical, trade-oriented or preparatory for gainful employment in a recognized occupation. 'Educational institution' includes, but is not limited to, community colleges and the public universities listed in ORS 352.002 but does not include kindergarten, elementary or secondary schools. (b) 'Social media' means an electronic medium that allows users to create, share and view user-generated content, including, but not limited to, uploading or downloading videos, still photographs, blogs, video blogs, podcasts, instant messages, electronic mail or Internet website profiles or locations. SECTION 2. Any person claiming to be aggrieved by a violation of section 1 of this 2013 Act may file a civil action in circuit court for equitable relief or, subject to the terms and conditions of ORS 30.265 to 30.300, damages, or both. The court may order such other relief as may be appropriate. Damages shall be $200 or actual damages, whichever is greater. (2) The action authorized by this section shall be filed within one year of the filing of a grievance. (3) An action under this section may not be filed unless, within 180 days of the alleged violation, a grievance has been filed with the governing body of the educational institution against which the violation is alleged. (4) An action under this section may not be filed until 90 days after filing a grievance unless only injunctive relief is sought pursuant to ORCP 79. The right to temporary or preliminary injunctive relief shall be independent of the right to pursue any
Utah

<table>
<thead>
<tr>
<th>Section</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>34-48-101. Title.</td>
<td>This chapter is known as the &quot;Internet Employment Privacy Act.&quot; Section 2. Section 34-48-102 is enacted to read: 34-48-102. Definitions. As used in this chapter: (1) &quot;Adverse action&quot; means to discharge, threaten, or otherwise discriminate against an employee in any manner that affects the employee's employment, including compensation, terms, conditions, location, rights, immunities, promotions, or privileges. (2) &quot;Employer&quot; means a person, including the state or a political subdivision of the state, that has one or more workers or operators employed in the same business or in or about the same establishment, under any contract of hire, express or implied, oral or written. (3) &quot;Law enforcement agency&quot; is as defined in Section 53-1-102. (4) (a) &quot;Personal Internet account&quot; means an online account that is used by an employee or applicant exclusively for personal communications unrelated to any business purpose of the employer. (b) &quot;Personal Internet account&quot; does not include an account created, maintained, used, or accessed by an employee or applicant for business related communications or for a business purpose of the employer. Section 3. Section 34-48-201 is enacted to read:</td>
</tr>
<tr>
<td>34-48-201. Employer may not request disclosure of information related to personal Internet account.</td>
<td>An employer may not do any of the following: (1) request an employee or an applicant for employment to disclose a username and password, or a password that allows access to the employee's or applicant's personal Internet account; or (2) take adverse action, fail to hire, or otherwise penalize an employee or applicant for employment failure to disclose information described in Subsection (1) or (2) of this section.</td>
</tr>
<tr>
<td>34-48-202. Permitted actions by an employer.</td>
<td>(1) This chapter does not prohibit an employer from doing any of the following: (a) requesting or requiring an employee to disclose a username or password required only to gain access to the following: (i) an electronic communications device supplied by or paid for in whole or in part by the employer; or (ii) an account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, and used for the employer's business purposes; (b) disciplining or discharging an employee for transferring the employer's proprietary or confidential information or financial data to an employee's personal Internet account without the employer's authorization; (c) conducting an investigation or requiring an employee to cooperate in an investigation in any of the following: (i) if there is specific information about activity on the employee's personal Internet account, for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct; or (ii) if the employer has specific information about an unauthorized transfer of the employer's proprietary information, confidential information, or financial data to an employee's personal Internet account; (d) restricting or prohibiting an employee's access to certain websites while using an electronic communications device supplied by, or paid for in whole or in part by, the employer while using an employer's network or resources, in accordance with state and federal law; or (e) monitoring, reviewing, accessing, or blocking electronic data stored on an electronic communications device supplied by, or paid for in whole or in part by, the employer, or stored on an employer's network, in accordance with state and federal law. (2) Conducting an investigation or requiring an employee to cooperate in an investigation as specified in Subsection (1)(c) includes requiring the employee to share the content that has been reported in order to make a factual determination. (3) This chapter does not prohibit or restrict an employer from complying with a duty to screen employees or applicants before hiring or to monitor or retain employee communications that is established under federal law, by a self-regulatory organization under the Securities and Exchange Act of 1934, 15 U.S.C. Sec. 78c(a)(26), or in the course of a law enforcement employment application or law enforcement officer conduct investigation performed by a law enforcement agency. (4) This chapter does not prohibit or restrict an employer from viewing, accessing, or using information about an employee or applicant that can be obtained without the information described in Subsection 34A-48-201(1) or that is available in the public domain. Section 5. Section 34-48203 is enacted to read:</td>
</tr>
<tr>
<td>34-48-203. Chapter does not create duties.</td>
<td>(1) This chapter does not create a duty for an employer to search or monitor the activity of a personal Internet account. (2) An employer is not liable under this chapter for failure to request or require that an employee or applicant for employment grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant for employment's personal Internet account. Section 6. Section 34-48-301 is enacted to read:</td>
</tr>
</tbody>
</table>
| 34-48-301. Private right of action. | (1) A person aggrieved by a violation of this chapter may bring a...
53B-24-101. Title. This chapter is known as the "Internet Postsecondary Institution Privacy Act."

53B-24-102. Definitions. As used in this chapter: (1) (a) "Personal Internet account" means an online account that is used by a student or prospective student exclusively for personal communications unrelated to any purpose of the postsecondary institution. (b) "Personal Internet account" does not include an account created, maintained, used, or accessed by a student or prospective student for education related communications or for an educational purpose of the postsecondary institution. (2) "Postsecondary institution" means an institution that provides educational services offered primarily to persons who have completed or terminated their secondary or high school education or who are beyond the age of compulsory school attendance. Section 9. Section 53B-24-201 is enacted to read:

53B-24-201. Prohibited activities. A postsecondary institution may not do any of the following: (1) request a student or prospective student to disclose a username and password, or a password that allows access to the student's or prospective student's personal Internet account; or (2) expel, discipline, fail to admit, or otherwise penalize a student or prospective student for failure to disclose information specified in Subsection (1).

53B-24-202. Permitted activities. (1) This chapter does not prohibit a postsecondary institution from requesting or requiring a student to disclose a username or password to gain access to or operate the following: (a) an electronic communications device supplied by or paid for in whole or in part by the postsecondary institution; or (b) an account or service provided by the postsecondary institution that is either obtained by virtue of the student's admission to the postsecondary institution or used by the student for educational purposes. (2) This chapter does not prohibit or restrict a postsecondary institution from viewing, accessing, or using information about a student or prospective student that can be obtained without the information described in Subsection 53B-24-201(1) or that is available in the public domain.

53B-24-203. Duties not created. (1) This chapter does not create a duty for a postsecondary institution to search or monitor the activity of a personal Internet account. (2) A postsecondary institution is not liable under this chapter for failure to request or require that a student or prospective student grant access to, allow observation of, or disclose information that allows access to or observation of the student's or prospective student's personal Internet account. Section 12. Section 53B-24-301 is enacted to read:

53B-24-301. Private right of action. (1) A person aggrieved by a violation of this chapter may bring a civil cause of action against a postsecondary institution in a court of competent jurisdiction. (2) In an action brought under Subsection (1), if the court finds a violation of this chapter, the court shall award the aggrieved person not more than $500.

### Vermont

4195. LEGISLATIVE FINDINGS AND STATEMENT OF PURPOSE

(a) The General Assembly finds that: (1) Vermont is striving to build an entrepreneurial and knowledge based economy. Attracting and nurturing small and medium sized internet technology ("IT") and other knowledge based companies is an important part of this effort and will be beneficial to Vermont's future. (2) Patents are essential to encouraging innovation, especially in the IT and knowledge based fields. The protections afforded by the federal patent system create an incentive to invest in research and innovation, which spurs economic growth. Patent holders have every right to enforce their patents when they are infringed, and patent enforcement litigation is necessary to protect intellectual property. (3) The General Assembly does not wish to interfere with the good faith enforcement of patents or good faith patent litigation. The General Assembly also recognizes that Vermont is preempted from passing any law that conflicts with federal patent law. (4) Patent litigation can be technical, complex, and expensive. The expense of patent litigation, which may cost hundreds of thousands of dollars or more, can be a significant burden on small and medium sized companies. Vermont wishes to help its businesses avoid these costs by encouraging the most efficient resolution of patent infringement claims without conflicting with federal law. (5) In order for Vermont companies to be able to respond promptly and efficiently to patent infringement assertions against them, it is necessary that they receive specific information regarding how their product, service, or technology may have infringed the patent at issue. Receiving such information at an early stage will facilitate the resolution of claims and lessen the burden of potential litigation on Vermont companies. (6) Abusive patent litigation, and especially the assertion of bad faith infringement claims, can harm Vermont companies. A business that receives a letter asserting such claims faces the threat of expensive and protracted litigation and may feel that it has no choice but to settle and to pay a licensing fee, even if the claim is meritless. This is especially so for small and medium sized companies and nonprofits that lack the resources to investigate and defend themselves against infringement claims. (7) Not only do bad faith patent infringement claims impose a significant burden on individual Vermont businesses, they also undermine Vermont’s efforts to attract and nurture small and medium sized IT and other knowledge
4196. DEFINITIONS In this chapter: (1) “Demand letter” means a letter, e-mail, or other communication asserting or claiming that the target has engaged in patent infringement. (2) “Target” means a Vermont person: (A) who has received a demand letter or against whom an assertion or allegation of patent infringement has been made; (B) who has been threatened with litigation or against whom a lawsuit has been filed alleging patent infringement; or (C) whose customers have received a demand letter asserting that the person’s product, service, or technology has infringed a patent.

4197. BAD FAITH ASSERTIONS OF PATENT INFRINGEMENT (a) A person shall not make a bad faith assertion of patent infringement. (b) A court may consider the following factors as evidence that a person has made a bad faith assertion of patent infringement: (1) The demand letter does not contain the following information: (A) the patent number; (B) the name and address of the patent owner or owners and assignee or assignees, if any; and (C) factual allegations concerning the specific areas in which the target’s products, services, and technology infringe the patent or are covered by the claims in the patent. (2) Prior to sending the demand letter, the person fails to conduct an analysis comparing the claims in the patent to the target’s products, services, and technology, or such an analysis was done but does not identify specific areas in which the products, services, and technology are covered by the claims in the patent. (3) The demand letter lacks the information described in subdivision (1) of this subsection, the target requests the information, and the person fails to provide the information within a reasonable period of time. (4) The demand letter demands payment of a license fee or response within an unreasonably short period of time. (5) The person offers to license the patent for an amount that is not based on a reasonable estimate of the value of the license. (6) The claim or assertion of patent infringement is meritless, and the person knew, or should have known, that the claim or assertion is meritless. (7) The claim or assertion of patent infringement is deceptive. (8) The person or its subsidiaries have previously filed or threatened to file one or more lawsuits based on the same or similar claim of patent infringement and: (A) those threats or lawsuits lacked the information described in subdivision (1) of this subsection; or (B) the person attempted to enforce the claim of patent infringement in litigation and a court found the claim to be meritless. (9) Any other factor the court finds relevant. (c) A court may consider the following factors as evidence that a person has not made a bad faith assertion of patent infringement: (1) The demand letter contains the information described in subdivision (b)(1) of this section. (2) Where the demand letter contains the information described in subdivision (b)(1) of this section and the target requests the information, the person provides the information within a reasonable period of time. (3) The person engages in a good faith effort to establish that the target has infringed the patent and to negotiate an appropriate remedy. (4) The person makes a substantial investment in the use of the patent or in the production or sale of a product or item covered by the patent. (5) The person is: (A) the inventor or joint inventor of the patent or, in the case of a patent filed by and awarded to an assignee of the original inventor or joint inventor, is the original assignee; or (B) an institution of higher education or a technology transfer organization owned or affiliated with an institution of higher education. (6) The person has: (A) demonstrated good faith business practices in previous efforts to enforce the patent, or a substantially similar patent; or (B) successfully enforced the patent, or a substantially similar patent, through litigation. (7) Any other factor the court finds relevant.

4198. BOND Upon motion by a target and a finding by the court that a target has established a reasonable likelihood that a person has made a bad faith assertion of patent infringement in violation of this chapter, the court shall require the person to post a bond in an amount equal to a good faith estimate of the target’s costs to litigate the claim and amounts reasonably likely to be recovered under § 4199(b) of this chapter, conditioned upon payment of any amounts finally determined to be due to the target. A hearing shall be held if either party so requests. A bond ordered pursuant to this section shall not exceed $250,000.00. The court may waive the bond requirement if it finds the person has available assets equal to the amount of the proposed bond or for other good cause shown.

4199. ENFORCEMENT; REMEDIES; DAMAGES (a) The Attorney General shall have the same authority under this chapter to make rules, conduct civil investigations, bring civil actions, and enter into assurances of discontinuance as provided under chapter 63 of this title. In an action brought by the Attorney General under this chapter the court may award any relief available under chapter 63 of this title. (b) A target of conduct involving assertions of patent infringement, or a person aggrieved by a violation of this chapter or by a violation of rules adopted under this chapter, may bring an action in Superior Court. A court may award the following remedies to a plaintiff who prevails in an action brought pursuant to this subsection: (1) equitable relief; (2) damages; (3) costs and fees, including reasonable attorney’s fees; and (4) exemplary damages in an amount equal to $50,000.00 or
### 49.44 RCW Section 1

<table>
<thead>
<tr>
<th>Washington</th>
<th>49.44 RCW Section 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) An employer may not: (a) Request, require, or otherwise coerce an employee or applicant to disclose login information for the employee's or applicant's personal social networking account; (b) Request, require, or otherwise coerce an employee or applicant to access his or her personal social networking account in the employer's presence in a manner that enables the employer to observe the contents of the account; (c) Compel or coerce an employee or applicant to add a person, including the employer, to the list of contacts associated with the employee's or applicant's personal social networking account; (d) Request, require, or cause an employee or applicant to alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account; or (e) Take adverse action against an employee or applicant because the employee or applicant refuses to disclose his or her login information, access his or her personal social networking account in the employer's presence, add a person to the list of contacts associated with his or her personal social networking account, or alter the settings on his or her personal social networking account that affect a third party's ability to view the contents of the account.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) This section does not apply to an employer's request or requirement that an employee share content from his or her personal social networking account if the following conditions are met: (a) The employer requests or requires the content to make a factual determination in the course of conducting an investigation; (b) The employer undertakes the investigation in response to receipt of information about the employee's activity on his or her personal social networking account; (c) The purpose of the investigation is to: (i) Ensure compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct; or (ii) Investigate an allegation of unauthorized transfer of an employer's proprietary information, confidential information, or financial data to the employee's personal social networking account; and (d) The employer does not request or require the employee to provide his or her login information.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(3) This section does not: (a) Apply to a social network, intranet, or other technology platform that is intended primarily to facilitate work-related information exchange, collaboration, or communication by employees or other workers; (b) Prohibit an employer from requesting or requiring an employee to disclose login information for access to: (i) An account or service provided by virtue of the employee's employment relationship with the employer; or (ii) An electronic communications device or online account paid for or supplied by the employer; (c) Prohibit an employer from enforcing existing personnel policies that do not conflict with this section; or (d) Prevent an employer from complying with the requirements of state or federal statutes, rules or regulations, case law, or rules of self-regulatory organizations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(4) If, through the use of an employer-provided electronic communications device or an electronic device or program that monitors an employer's network, an employer inadvertently receives an employee's login information, the employer is not liable for possessing the information but may not use the login information to access the employee's personal social networking account.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(5) For the purposes of this section and section 2 of this act: (a) &quot;Adverse action&quot; means: Discharging, disciplining, or otherwise penalizing an employee; threatening to discharge, discipline, or otherwise penalize an employee; and failing or refusing to hire an applicant.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(b) &quot;Applicant&quot; means an applicant for employment. (c) &quot;Electronic communications device&quot; means a device that uses electronic signals to create, transmit, and receive information, including computers, telephones, personal digital assistants, and other similar devices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(d) &quot;Employer&quot; means any person, firm, corporation, partnership, business trust, legal representative, or other business entity which engages in any business, industry, profession, or other activity in this state and employs one or more employees, and includes the state, any state institution, state agency, political subdivisions of the state, and any municipal corporation or quasi-municipal corporation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;Employer&quot; includes an agent, a representative, or a designee of the employer. (e) &quot;Login information&quot; means a user name and password, a password, or other means of authentication that protects access to a personal social networking account. Section 2. An employee or applicant aggrieved by a violation of section 1 of this act may bring a civil action in a court of competent jurisdiction. The court may: (1) Award a prevailing employee or applicant injunctive or other equitable relief, actual damages, a penalty in the amount of five hundred dollars, and reasonable attorneys' fees and costs; and (2) Pursuant to RCW 4.84.185, award any prevailing party against whom an action has been brought for a violation of section 1 of this act reasonable expenses and attorneys' fees upon final judgment and written findings by the trial judge that the action was frivolous and advanced without reasonable cause.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>