

AN ACT concerning employment.

**Be it enacted by the People of the State of Illinois,  
represented in the General Assembly:**

Section 5. The Freedom From Location Surveillance Act is amended by changing Section 5 as follows:

(725 ILCS 168/5)

Sec. 5. Definitions. For the purpose of this Act:

"Basic subscriber information" means name, address, local and long distance telephone connection records or records of session time and durations; length of services, including start dates, and types of services utilized; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and the means and source of payment for the service, including the credit card or bank account number.

"Electronic device" means any device that enables access to, or use of:

(1) an electronic communication service that provides the ability to send or receive wire or electronic communications;

(2) a remote computing service that provides computer storage or processing services by means of an electronic communications system; or

(3) a location information service such as a global positioning service or other mapping, locational, or directional information service.

"Electronic device" does not mean devices used by a governmental agency or by a company operating under a contract with a governmental agency for toll collection, traffic enforcement, or license plate reading.

"Law enforcement agency" means any agency of this State or a political subdivision of this State which is vested by law with the duty to maintain public order or enforce criminal laws.

"Location information" means any information concerning the location of an electronic device that, in whole or in part, is generated by or derived from the operation of that device.

"Social networking website" has the same meaning ascribed to the term in ~~paragraph (4) of~~ subsection (b) of Section 10 of the Right to Privacy in the Workplace Act.

(Source: P.A. 98-1104, eff. 8-26-14.)

Section 10. The Right to Privacy in the Workplace Act is amended by changing Section 10 as follows:

(820 ILCS 55/10) (from Ch. 48, par. 2860)

Sec. 10. Prohibited inquiries; online activities.

(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 or prospective employer to:

(A) request, ~~or~~ require, or coerce any employee or prospective employee to provide a user name and password or any password or other related account information in order to gain access to the employee's or prospective employee's personal online account ~~or profile on a social networking website~~ or to demand access in any manner to an employee's or prospective employee's personal online account; ~~or profile on a social networking website.~~

(B) request, require, or coerce an employee or applicant to authenticate or access a personal online account in the presence of the employer;

(C) require or coerce an employee or applicant to invite the employer to join a group affiliated with any personal online account of the employee or applicant;

(D) require or coerce an employee or applicant to join an online account established by the employer or add the employer or an employment agency to the employee's or applicant's list of contacts that enable the contacts to access the employee or applicant's personal online

account;

(E) discharge, discipline, discriminate against, retaliate against, or otherwise penalize an employee for (i) refusing or declining to provide the employer with a user name and password, password, or any other authentication means for accessing his or her personal online account, (ii) refusing or declining to authenticate or access a personal online account in the presence of the employer, (iii) refusing to invite the employer to join a group affiliated with any personal online account of the employee, (iv) refusing to join an online account established by the employer, or (v) filing or causing to be filed any complaint, whether orally or in writing, with a public or private body or court concerning the employer's violation of this subsection; or

(F) fail or refuse to hire an applicant as a result of his or her refusal to (i) provide the employer with a user name and password, password, or any other authentication means for accessing a personal online account, (ii) authenticate or access a personal online account in the presence of the employer, or (iii) invite the employer to join a group affiliated with a personal online account of the applicant.

(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; or ~~and~~

(B) monitor usage of the employer's electronic equipment and the employer's electronic mail without requesting or using ~~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 personal online account ~~or profile on a social networking website.~~

(3) Nothing in this subsection shall prohibit an employer from:

(A) 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;

(B) complying with State and federal laws, rules, and regulations and the rules of self-regulatory organizations created pursuant to federal or State law when applicable;

(C) requesting or requiring an employee or applicant to share specific content that has been reported to the employer, without requesting or requiring an employee or applicant to provide a user name and password, password, or other means of authentication that provides access to an employee's or applicant's personal online account, for the purpose of:

(i) ensuring compliance with applicable laws or regulatory requirements;

(ii) investigating an allegation, based on receipt of specific information, of the unauthorized transfer of an employer's proprietary or confidential information or financial data to an employee or applicant's personal account;

(iii) investigating an allegation, based on receipt of specific information, of a violation of applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct;

(iv) prohibiting an employee from using a personal online account for business purposes; or

(v) prohibiting an employee or applicant from accessing or operating a personal online account during business hours, while on business property, while using an electronic communication device supplied by, or paid for by, the employer, or while using the employer's network or resources, to the extent permissible under applicable laws.

(4) If an employer inadvertently receives the username, password, or any other information that would enable the employer to gain access to the employee's or potential employee's personal online account through the use of an otherwise lawful technology that monitors the employer's network or employer-provided devices for network security or

data confidentiality purposes, then the employer is not liable for having that information, unless the employer:

(A) uses that information, or enables a third party to use that information, to access the employee or potential employee's personal online account; or

(B) after the employer becomes aware that such information was received, does not delete the information as soon as is reasonably practicable, unless that information is being retained by the employer in connection with an ongoing investigation of an actual or suspected breach of computer, network, or data security. Where an employer knows or, through reasonable efforts, should be aware that its network monitoring technology is likely to inadvertently to receive such information, the employer shall make reasonable efforts to secure that information.

(5) 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) provided ~~(3.5) Provided~~ that the password, account information, or access sought by the employer only relates to an online account that:

(A) an employer supplies or pays; or

(B) an employee creates or maintains on behalf of or

~~under direction of an employer in connection with that employee's employment. 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).~~

(6) ~~(4)~~ For the purposes of this subsection:~~7~~

(A) "Social ~~social~~ networking website" means an Internet-based service that allows individuals to:

(i) ~~(A)~~ construct a public or semi-public profile within a bounded system, created by the service;

(ii) ~~(B)~~ create a list of other users with whom they share a connection within the system; and

(iii) ~~(C)~~ view and navigate their list of connections and those made by others within the system.

"Social networking website" does ~~shall~~ not include electronic mail.

(B) "Personal online account" means an online account, that is used by a person primarily for personal purposes. "Personal online account" does not include an account created, maintained, used, or accessed by a person for a business purpose of the person's employer or prospective



employer.

~~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.~~

(Source: P.A. 97-875, eff. 1-1-13; 98-501, eff. 1-1-14.)