

WEST VIRGINIA LEGISLATURE

2016 REGULAR SESSION

Introduced

House Bill 4364

(BY DELEGATES SKINNER, MCGEEHAN, HAMRICK,
FLUHARTY, HOUSEHOLDER, BLAIR, SPONAUGLE,
MANCHIN, MILEY, BYRD AND MARCUM)

[Introduced February 2, 2016; Referred
to the Committee on the Judiciary.]

1 A BILL to amend the Code of West Virginia, 1931, as amended, by adding thereto a new article,
 2 designated §21-5G-1, §21-5G-2, §21-5G-3 and §21-5G-4, all relating to employment and
 3 privacy protection; prohibiting an employer from requesting or requiring that an employee
 4 or applicant disclose any user name, password, or other means for accessing a personal
 5 account or service through certain electronic communications devices; prohibiting an
 6 employer from taking or threatening to take, certain disciplinary actions for an employee's
 7 refusal to disclose certain password and related information; prohibiting an employer from
 8 failing or refusing to hire an applicant as a result of the applicant's refusal to disclose
 9 certain password and related information; prohibiting an employee from downloading
 10 certain unauthorized information or data to certain websites or web-based accounts;
 11 providing that an employer is not prevented from conducting certain investigations for
 12 certain purposes, including gathering information needed for compliance with mandatory
 13 state or federal regulations; and duties not created under this article.

Be it enacted by the Legislature of West Virginia:

1 That the Code of West Virginia, 1931, as amended, be amended by adding thereto a new
 2 article, designated §21-5G-1, §21-5G-2, §21-5G-3 and §21-5G-4, all to read as follows:

ARTICLE 5G. INTERNET PRIVACY PROTECTION ACT.

§21-5G-1. Short Title.

1 This article shall be known and may be cited as the "Internet Privacy Protection Act".

§21-5G-2. Definitions.

1 As used in this article:

2 (1) "Applicant" means an applicant for employment.

3 (2) "Electronic Communications Device" means any device that uses electronic signals to
 4 create, transmit and receive information, and includes computers, telephones, personal digital
 5 assistants, and other similar devices.

6 (3) "Employer" means a person engaged in a business, industry, profession, trade or other
7 enterprise in the state, or a unit of state or local government. "Employer" includes an agent,
8 representative or designee of the employer.

§21-5G-3. Certain acts prohibited; not prohibited.

1 (a) An employer may not request or require that an employee or applicant disclose any
2 user name, password, or other means for accessing a personal account or service through an
3 electronic communications device.

4 (b) (1) An employer may not discharge, discipline, or otherwise penalize or threaten to
5 discharge, discipline, or otherwise penalize an employee for the employee's refusal to disclose
6 any information specified in subsection (a) of this section.

7 (2) An employer may not fail or refuse to hire any applicant as a result of the applicant's
8 refusal to disclose any information specified in subsection (a) of this section.

9 (c) An employee may not download any information not authorized by the employer,
10 including, but not limited to, proprietary information, trade secrets, or financial data to an
11 employee's personal website, an Internet website, a web-based account or a similar account, or
12 to any other electronic or digital storage device or medium.

13 (d) (1) This section does not prevent an employer, based on the receipt of information
14 about the use of a personal website, Internet website, web-based account, or similar account by
15 an employee for business purposes, from conducting an investigation for the purpose of ensuring
16 compliance with applicable securities or financial law, or regulatory requirements.

17 (2) This section does not prohibit an employer from doing any of the following:

18 (A) Requesting or requiring an employee to disclose a username or password to gain
19 access to:

20 (i) An electronic communications device where the costs of the device and the charges for
21 the use thereof are primarily paid by the employer; or

22 (ii) An account or service provided by the employer or obtained by virtue of the employee's
23 employment relationship with the employer, and used for the employer's business purposes;

24 (B) Disciplining or discharging an employee for transferring the employer's proprietary or
25 confidential information or financial data to an employee's personal Internet account without the
26 employer's authorization;

27 (C) Conducting an investigation or requiring an employee to cooperate in an investigation
28 in any of the following:

29 (i) If there is specific information about activity, relating to the employment of the individual
30 or the business of the employer, on the employee's personal Internet account, for the purpose of
31 ensuring compliance with applicable laws, regulatory requirements or written employee codes of
32 conduct found within previously known and agreed to written employee contracts; or

33 (ii) If the employer has specific information about an unauthorized transfer of the
34 employer's proprietary information, confidential information or financial data to an employee's
35 personal Internet account;

36 (D) Restricting or prohibiting an employee's access to certain websites while using an
37 electronic communications device where the costs of the device and the charges for the use
38 thereof are primarily paid by the employer or while using an employer's network or resources, in
39 accordance with state or federal law;

40 (E) Monitoring, reviewing, accessing or blocking electronic data stored on an electronic
41 communications device where the costs of the device and the charges for the use thereof are
42 primarily paid by the employer or stored on an employer's network, in accordance with state and
43 federal law; or

44 (F) Conducting an investigation or requiring an employee to cooperate in an investigation
45 as specified in subsection (2)(c), including requiring the employee to share the content that has
46 been reported in order to make a factual determination.

47 (3) This section does not prohibit or restrict an employer from complying with a duty to
48 screen employees or applicants before hiring or to monitor or retain employee communications
49 that is established under federal law, by a self-regulatory organization under the Securities and

50 Exchange Act of 1934, 15 U.S.C. Sec. 78c(a)(26), or in the course of a law enforcement
 51 employment application or law-enforcement officer investigation performed by a law-enforcement
 52 agency.

53 (4) This section does not prohibit or restrict an employer from viewing, accessing or using
 54 information about an employee or applicant that can be obtained without the information
 55 described in §21-5G-3(a) or information available in the public domain.

§21-5G-4. Duties not created.

1 (a) This article does not create a duty for an employer to search or monitor the activity of
 2 a personal Internet account.

3 (b) An employer is not liable under this article for failure to request or require that an
 4 employee or applicant for employment grant access to, allow observation of or disclose
 5 information that allows access to or observation of the applicant or employee’s personal Internet
 6 account.

NOTE: The purpose of this bill is to protect the privacy of personal electronic data for employees and applicants for employment, and to authorize employers to investigate to ensure compliance with applicable protections of certain business information.

Strike-throughs indicate language that would be stricken from a heading or the present law, and underscoring indicates new language that would be added.