jackson lewis
all we do is work

Michigan Bars Employers from Demanding Private Social Media Information from Applicants, Employees

Date: 1.10.2013

A new Michigan law signed by Governor Rick Snyder prohibits employers and prospective employers from requiring employees and applicants to grant access to, allow observation of, or disclose information used to access private Internet and e-mail accounts, including social media networks such as Facebook. This ban also applies to educational institutions and their students. Michigan's Internet Privacy Protection Act, Public Act 478 of 2012, is effective as of December 28, 2012. The new law also prohibits employers from discharging, disciplining, failing to hire, or otherwise penalizing those who refuse to disclose information that allows access to such accounts.

A covered employer under the law is "a person, including a unit of state or local government, engaged in a business, industry, profession, trade, or other enterprise in this state and includes an agent, representative, or designee of the employer." A person who violates the Act is guilty of a misdemeanor punishable by a fine of not more than $1,000.

The Act does not prohibit an employer from doing any of the following:

(a) Requesting or requiring an employee to disclose access information to the employer to gain access to or operate any of the following:

(i) An electronic communications device paid for in whole or in part by the employer.

(ii) An account or service provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or 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 circumstances:

(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.

(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 paid for in whole or in part by the employer or while using an employer's network or resources, in accordance with state and federal law.

(e) Monitoring, reviewing, or accessing electronic data stored on an electronic communications device paid for in whole or in part by the employer, or traveling through or stored on an employer's network, in accordance with state and federal law.

In addition, the Act does not 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 that is established under federal law or by a self regulatory organization, as defined in section 3(a)(26) of the securities and exchange act of 1934, 15 USC 78c(a)(26).

Finally, the Act does not prohibit or restrict an employer from viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain.

If you have any questions about this or other workplace developments, please contact Marlo Johnson Roebuck, at (248) 936-1900 or RoebuckM@jacksonlewis.com, or the Jackson Lewis attorney with whom you regularly work.

---

practices

Management Education

Privacy, Social Media and Information Management