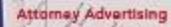


The logo for Robinson+Cole, with the plus sign in green.

Labor + Employment

A blue cover of an 'EMPLOYEE HANDBOOK' with a white geometric pattern.A small red text box in the top right corner of the header image that says 'Attorney Advertising'.

May 2015

Connecticut Employers Must Soon Comply with New Social Media Privacy Law

Connecticut has enacted a new law, Public Act 15-6, that restricts employers' ability to access personal online accounts of employees and applicants. A "personal online account" is defined as an account used exclusively by an employee or applicant for personal purposes and unrelated to any business purpose of such employee's or applicant's employer or prospective employer, including, but not limited to, electronic mail, social media, and retail-based Internet websites. It does not, however, include any account created, maintained, used, or accessed by an employee or applicant for a business purpose of the employer or prospective employer.

The new law prohibits employers from the following:

1. Requesting or requiring that an employee or applicant provide the employer with a username and/or password or any other authentication means for accessing a personal online account
2. Requesting or requiring that an employee or applicant authenticate or access a personal online account in the presence of the employer
3. Requiring that an employee or applicant invite the employer or accept an invitation from the employer to join a group affiliated with any personal online account of the employee or applicant
4. Discharging, disciplining, discriminating against, retaliating against, or otherwise penalizing any employee who refuses to provide the employer with the means for accessing a personal online account
5. Failing or refusing to hire any applicant who refuses to provide the employer with access to a personal online account

The law does not prohibit an employer from requesting or requiring access to an account or service provided by the employer for the employer's business purposes. Further, an employer may request or require an employee or applicant to provide a username and password or any other authentication means for accessing any electronic communications device supplied or paid for, in whole or in part, by the employer. The law also does not preclude an employer from monitoring, reviewing, accessing, or blocking electronic data stored on an electronic communications device paid for, in whole or in part, by an employer or traveling through or stored on an employer's network, in compliance with state and federal law.

In addition, the law allows an employer to fire, discipline, or otherwise penalize an employee who has

transferred an employer's proprietary, confidential, or financial information to or from a personal online account. Similarly, employers are allowed under the law to conduct an investigation for ensuring compliance with state and federal laws or for employee misconduct based on information received about an employee's online conduct or misappropriation of employer data.

Complaints that an employer has violated the law can be filed with the state labor commissioner, who will investigate and may conduct a hearing. Any employee or applicant who prevails in such a hearing will be awarded reasonable attorney's fees and costs. Further, the commissioner may levy a civil penalty of up to \$500 for the first violation, and \$1,000 for each subsequent violation, and award the employee appropriate relief, including rehiring, back wages, benefits, or "any other remedies that the commissioner may deem appropriate." The commissioner may also request that the attorney general bring an action in Superior Court to recover penalties levied against the employer.

The law will go into effect on October 1, 2015. In advance of the effective date, employers may want to review their policies and practices concerning e-mail, social media, and similar online activities to ensure they are in compliance.

For more information, please contact any of the following members of
Robinson+Cole's [Labor, Employment, Benefits + Immigration Group](#):

[Stephen W. Aronson](#) | [Ian T. Clarke-Fisher](#) | [Britt-Marie K. Cole-Johnson](#) | [Peter A. Dagostine](#)
[Alice E. DeTora](#) | [Natale V. Di Natale](#) | [Katherine C. Glynn](#) | [Sandra Marin](#) | [Susan N. Masters](#)
[Matthew T. Miklave](#) | [Nicole H. Najam](#) | [Jean E. Tomasco](#)

Or please reach out to [Linn F. Freedman](#), chair of our
[Data Privacy and Security Team](#) or any other member of the team.

For insights on legal issues affecting various industries,
please visit our [Thought Leadership](#) page and subscribe to any of our newsletters or blogs.

[Boston](#) | [Hartford](#) | [New York](#) | [Providence](#) | [Stamford](#) | [Albany](#) | [Los Angeles](#) | [Miami](#) | [New London](#) | [rc.com](#)

© 2015 Robinson & Cole LLP. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission. This document should not be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.