Proskauer

special report

Social Media Roundup

in this issue

AUGUST 2014

By Katharine H. Parker, Daniel L. Saperstein, Harry N. Hudesman and Allison L. Martin

Social Media Roundup

Rhode Island, Louisiana, New Hampshire, and Oklahoma are the latest states to provide prospective and/or current employees with increased social media protections, following Tennessee, Wisconsin, New Jersey, Maryland, Illinois, California, Michigan, Utah, New Mexico, Arkansas, Colorado, Washington, Oregon and Nevada. This special report highlights the key provisions of the new laws and examines the implications for covered employers.

Rhode Island

Rhode Island's new social media law, which took effect on June 30, 2014, covers any person in the state employing individuals or acting in the interest of an employer. Under the new Rhode Island law, employers may not require, coerce or request an employee or applicant to:

- disclose the password or any other means of access to a personal social media account;[1]
- access a personal social media account in the presence of the employer or representative; or
- divulge personal social media account information, unless the employer reasonably believes the information is relevant to an investigation into alleged employee misconduct or workplace-related violations of applicable laws and regulations, and when not otherwise prohibited by law or constitution. (The information only may be accessed and used to the extent necessary for that investigation or a related proceeding).

[1] Under the new Rhode Island law, a "social media account" is 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 service or accounts, or Internet website profiles or locations.

Employers also may not:

- compel an employee or applicant to add anyone, including the employer or its agent, to a list of contacts associated with a personal social media account; or
- require, request or cause an employee or applicant to alter the settings that affect a third party's ability to view the contents of a personal social media account.

Additionally, an employer may not take, or threaten to take, an adverse employment action against an employee or applicant who refuses to disclose or provide access to a personal social media account, add the employer as a social media contact, or alter the settings associated with a personal social media account.

Despite these prohibitions, the new Rhode Island law allows an employer to access publically available information about an employee or applicant. It also does not prohibit or restrict an employer from complying with a duty to screen employees or applicants before hiring, or to retain employee communications, when that duty is established by a self-regulatory organization (as defined by the Securities Exchange Act) or state or federal law or regulation (to the extent necessary to supervise communications of regulated financial institutions insurance or securities licensees for bank insurance or securities-related business purposes).

The new Rhode Island law allows for a civil action to recover damages and reasonable attorneys' fees and costs, in addition to declaratory and injunctive relief.

Louisiana

The new Louisiana law, which took effect on August 1, 2014, covers any person engaged in a business, industry, profession, trade or other enterprise in Louisiana, and an agent, representative or designee of such an employer. Under the new Louisiana law, an employer may not require an employee or applicant to disclose any username, password, or other authentication information (hereinafter, "authentication information") that allows access to the individual's personal online account.[2] The new law also prohibits an employer from taking, or threatening to take, adverse action against a prospective or current employee for refusing to disclose authentication information to his personal online account.

Despite these prohibitions, the new Louisiana law permits employers to:

- request or require an employee or applicant to disclose authentication information for the purpose of accessing (i) an electronic communications device[3] paid for or supplied 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 or applicant's relationship with the employer, or used for the employer's business purposes;

---

[2] Louisiana's new law defines a "personal online account" as one that the employee or applicant uses exclusively for personal communications unrelated to any business purpose of the employer.

[3] Louisiana's new law defines an "electronic communications device" as one that uses electronic signals to create, transmit, and receive information, including a computer, telephone, personal digital assistant, or other similar device.

- discipline or discharge an employee for transferring the employer's proprietary, confidential, or financial information to an employee's personal online account without the employer's authorization;
- conduct an investigation (or require an employee or applicant to cooperate in an investigation) if there is "specific information" concerning activity on the employee's personal online account: (i) for the purpose of ensuring compliance with applicable laws, regulations or prohibition against work-related misconduct; or (ii) about the unauthorized transfer of the employer's proprietary, confidential, or financial information;
- conduct an investigation or require an employee or applicant to cooperate in an investigation (including requiring an employee or applicant to share the reported content in order to make a factual determination), without obtaining authentication information to his personal online account;
- restrict or prohibit an employee's or applicant's access to certain websites while using an electronic communications device paid for or supplied in whole or in part by the employer or while using the employer's network or resources, in accordance with state and federal law;
- comply with a duty to screen employees or applicants, or monitor or retain employee communications, pursuant to a federal or state law, rule, regulation, case law, or rules of a self-regulatory organization;
- view, access or utilize information about an employee or applicant that can be obtained without the individual's authentication information, or that is available in the public domain; or
- require an employee to provide a personal e-mail address to facilitate employment-related communications in the event the employer's e-mail system fails.

Also, if an employer inadvertently obtains an employee's or applicant's authentication information through the use of an electronic device or program that monitors an employer's network or employer-provided device, it will not be held liable for possessing the information. (The employer still may not use the information to access the account.) Further, the new law does not prevent an employee or applicant from self-disclosing authentication information to allow the employer access to his personal online account.

Finally, the new Louisiana law makes clear that it does not create a duty for an employer to search or monitor the activity of an individual's personal online account. Along those lines, an employer will not be held liable for failing to request or require an applicant or employee to disclose authentication information to his personal online account. The new Louisiana law, however, does not specify what remedies would result if an employer were to violate the statute.

New Hampshire

New Hampshire's new social media law takes effect on September 30, 2014, and prohibits employers from:

- requesting or requiring that an employee or an applicant disclose login information used to access any personal account[4] or service through an electronic communication device;
- compelling an employee or applicant to add anyone, including the employer (or its agent), to a list of contacts associated with an e-mail account or personal account; or
- requiring an employee or applicant to reduce the privacy settings associated with any e-mail or personal account that would affect a third party's ability to view the contents of the account.

An employer also may not take (or threaten to take) disciplinary action against any employee for refusing to comply with a request or demand to violate the new law.

Despite these prohibitions, the new law does not limit an employer's right to:

- adopt and enforce lawful workplace policies governing the use of the employer's electronic equipment such as the Internet, a social networking site, and e-mail;
- monitor use of the employer's electronic equipment and e-mail;
- request or require an employee to disclose login information to access: (i) an account or service provided by virtue of the employee's employment relationship; or (ii) an electronic communications device or online account paid for or supplied by the employer;
- obtain information about an employee or prospective employee that is part of the public domain;
- conduct an investigation based on the receipt of specific information about activity on an employee's personal social media account or service received from an employee or other source:[5] (i) to ensure compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct; or (ii) concerning the unauthorized transfer of an employer's proprietary, confidential, or financial information; or
- otherwise comply with state or federal law, rules or regulations, case law, or the rules of a self-regulatory organization.

Also, if an employer inadvertently receives an employee's password or other authentication information through the use of an electronic device or program that monitors an employer's network or through the use of employer-provided devices, it is not liable for possessing this information. However, the employer may not use this information to access the account.

---

[4] New Hampshire's new law defines a "personal account" as an account, service, or profile on a social networking website used by a current or prospective employee primarily for personal communications unrelated to any business purposes of the employer.

[5] Under New Hampshire's new law, as part of the investigation, the employer may require the employee's cooperation to share only the content that it has received in order to make a factual determination.

Finally, New Hampshire's new law empowers the state labor commissioner to fine employers no more than $2,500 for violating the statute, subject to appeal.

Oklahoma

The new Oklahoma law, which takes effects on November 1, 2014, covers employers that (i) pay at least one individual with a salary or wages, or (ii) contract or subcontract with the state (or its agencies) to furnish material or perform work. Under the new Oklahoma law, an employer may not require an employee or prospective employee to:

- disclose a user name and password or other means of authentication (hereinafter, "authentication information") for accessing a personal online social media account[6] through an electronic communications device[7]; or
- access his or her personal online social media account in a manner that allows the employer to observe contents of the account otherwise shielded from the general public (unless the access is pursuant to an investigation permitted under the new law).

The new Oklahoma law also prohibits an employer from taking an adverse employment action against a prospective or current employee for refusing to provide authentication information to his personal online social media account.

Despite these prohibitions, the new Oklahoma law permits employers to:

- request or require an employee to disclose authentication information for the purpose of accessing (i) any computer system, information technology network, or electronic communications device provided or subsidized by the employer; or (ii) any accounts or services provided by the employer or by virtue of the employee's employment relationship, or that the employee uses for business purposes;
- conduct an investigation based on the receipt of specific information about activity on a personal online social media account or service by an employee or other source: (i) to ensure compliance with applicable laws, regulatory requirements or prohibitions against work-related employee misconduct, or (ii) concerning the unauthorized transfer of an employer's proprietary, confidential, or financial information;[8]
- comply with state or federal statutes, rules or regulations, case law, or rules of self-regulatory organizations;
- access the employer's computer system or information technology network, including electronic communications devices owned by the employer; or

---

[6] The new Oklahoma law defines a "personal online social media account" as one used by an employee or prospective employee exclusively for personal communications through such electronic applications as videos, still photographs, blogs, video blogs, instant messages, audio recordings or email that is not available to the general public.

[7] Under the new Oklahoma law, "electronic communications device" is one that uses electronic signals to create, transmit or receive information, including computers, telephones, personal digital assistants and other similar devices.

[8] Under the new Oklahoma law, "conducting an investigation" includes requiring the employee's cooperation to share the reported content in order to make a factual determination.

- review or access personal online social media accounts that an employee chooses to use while utilizing an employer's computer system, information technology network or electronic communication device;

If, through the use of an electronic device or program that monitors an employer's network or the use of employer provided devices, an employer inadvertently obtains an employee's authentication information, it is not liable for possessing such information. (The employer still may not use the information to access the account.) An employer also will not be held liable for *not* requesting, accessing, or reviewing an employee's personal online social media accounts.

Within six months of an alleged violation of the new Oklahoma law, an employee or prospective employee may bring a civil action for injunctive relief and damages not exceeding five hundred dollars per violation (punitive or emotional damages are not available under the statute). A violation of the new Oklahoma law also may not become the basis for a public policy tort.

Takeaway

To ensure compliance with the new law, employers in Rhode Island, Louisiana, New Hampshire, and Oklahoma should review their hiring, monitoring, and investigatory procedures regarding the use of social media, and make any necessary changes. Employers in these states also should be aware that engaging in the type of conduct the new laws prohibit may violate other laws such as the federal Stored Communications Act, as well as common law privacy rights. Furthermore, although the new laws permit employers to view publically accessible profiles, employers should recognize that such conduct may give rise to a discrimination claim under Title VII of the Civil Rights Act of 1964 or a state equivalent if the employer takes adverse action based on information that reveals a protected characteristic such as race or religion. Given these risks, employers in these states should adopt a clear and compliant workplace policy governing the use of social media.

Dubbed a “powerhouse” by *Chambers USA* and “amazing strategists” with “fantastic technical know-how” by *Chambers Europe*, our Labor & Employment Law Department is one of the strongest practices in the world with over 160 lawyers across the U.S., London and Paris offices. Indeed, we were ranked higher in more categories than any other labor practice in *US Legal 500* and received similar rankings from *Chambers USA* and *Chambers Europe*.

If you have any questions regarding the matters discussed in this newsletter, please contact any of the lawyers listed below:

Katharine H. Parker, Partner
212.969.3009 – kparker@proskauer.com

Allan H. Weitzman, Partner
561.995.4760 – aweitzman@proskauer.com

Marc A. Mandelman, Senior Counsel
212.969.3113 – mmandelman@proskauer.com

Fredric C. Leffler, Senior Counsel
212.969.3570 – fleffler@proskauer.com

Daniel L. Saperstein, Associate
973.274.3272 – dsaperstein@proskauer.com