US patchwork of social media laws creates confusion

Social media protection laws provide a cautionary tale and challenges for multinational employers. By **Phillip L. Gordon** and **William J. Simmons**.

Between March 2012 and August 2013, 12 states in the United States enacted so-called "social media password protection" legislation, designed to bar employers from, at a minimum, demanding the log-in credentials for applicants' and employees' private social media accounts. This flood of new legislation appears to have been unleashed in response to media reports of a few incidents where employers allegedly requested or required log-in credentials from job applicants.[1] Ironically, surveys of hundreds of senior executives and in-house employment counsel at US organizations conducted in June 2012 and June 2013 by the US law firm, Littler Mendelson, reported that 99% of the responding organizations did not ask applicants for their personal, social media log-in credentials.[2]

Despite the narrow scope and questionable nature of the purported problem, legislators in nearly all of the twelve states enacted prohibitions far broader than a restriction on requests for log-in credentials. Moreover, these new laws do not follow a model. Rather, they utilize different key terms (defined or undefined), feature varying prohibitions, and provide unique defenses, exceptions and enforcement provisions. The United States Congress has yet to enact any federal legislation that would preempt the states' laws in their entirety; consequently, the twelve states have created a complex legislative patchwork that defies attempts by multistate and multinational employers to implement a uniform policy to comply with these laws. This legislative morass creates significant challenges for organizations with employees in the relevant states and provides a cautionary tale for other countries considering similar legislation.

Range of employer conduct covered by the laws

The 12 states that have passed legislation – Arkansas, California, Colorado, Illinois, Maryland, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah and Washington – prohibit a range of employer conduct.

Although the laws are commonly referred to as "social media" password protection legislation, several of the laws protect sites or accounts besides those commonly understood to be social media sites, such as Facebook, Twitter and LinkedIn. For instance, the laws in Arkansas, California, Colorado, Maryland, Michigan, Nevada and Utah appear to cover any Internet-based personal account, even email accounts such as Gmail or Hotmail. Illinois' law covers accounts and profiles on "social networking websites," and Washington's law applies to "social networking accounts," but neither state defines "social networking." Oregon, New Mexico, and New Jersey appear to limit their laws' coverage to accounts commonly regarded as social media, although their defining language is vague.

Regardless of the type of Internet accounts covered by each law, all of these laws prohibit employers from asking applicants for their username, password or other log-in credentials, and all states except New Mexico impose the same basic restriction on requests to employees. The uniformity ends there. As summarized below, many of the twelve states have adopted the following additional prohibitions:

1. Prohibition on observing information in covered accounts after the individual has logged into the account, also known as "shoulder surfing" (California, Illinois, Maryland, Michigan, New Jersey, Oregon and Washington);
2. Prohibition on requiring the individual to accept the employer's "friend" or "connection" request (Arkansas, Colorado, Oregon and Washington);[3]
3. Prohibition on requiring the individual to change privacy settings to allow the employer to view information in the account that was previously restricted from public view (Arkansas, Colorado and Washington)[4]; and
4. Prohibition on requiring that an individual access for the employer the information in a covered account of another person to which the individual has access (California, Michigan and possibly New Jersey).

Each prohibition is subject to exceptions, which appear to reflect a general acceptance among the states' legislators that employers have legitimate business reasons to access a restricted social media account on certain occasions. For example, an employee may be using a restricted account to conduct business on the employer's behalf; an employer may have a legal obligation under securities laws to monitor an employee's public statements; or an employer may need access to restricted social media to investigate suspected misappropriation of trade secrets, a threat of workplace violence or other misconduct. Despite the apparent general recognition of employers' interests, the exceptions to these laws' prohibitions vary substantially from state to state as reflected in the summary of exceptions below:

1. An exception for accounts that are used for the business purposes of the employer (though the exception varies in scope depending on the state; all states have some version of this exception except for New Mexico because New Mexico's law applies only to job applicants);
2. An exception allowing access to an employee's covered account where necessary for a workplace

investigation (Arkansas, California, Michigan, New Jersey and Utah have a relatively broad exception; Colorado, Maryland, Oregon and Washington have a relatively narrow exception);

3. An exception allowing access to an employee's covered account where necessary to comply with obligations imposed by law or by the rules of a self-regulatory organization, such as the Financial Industry Regulatory Authority's (FINRA) rules on supervision of online communications (Arkansas, Illinois, Michigan, Nevada, Oregon, Utah and Washington);
4. An exception allowing an employer to acquire inadvertently an employee's log-in credentials to a covered account through routine monitoring of corporate electronic resources as long as the employer does not actually use the information to access the employee's covered account (Arkansas, Oregon and Washington); and
5. An exception for social media content that is publicly available (Arkansas, Illinois, Michigan, New Jersey, New Mexico, Oregon and Utah).

Regarding enforcement, while all states provide that a violation constitutes an unlawful employment practice, the enforcement schemes vary substantially among the states. Some states permit only administrative enforcement (California, Colorado and New Jersey). Other states also permit a private lawsuit (Illinois, Maryland, Michigan, Utah, Oregon and Washington). Among those states, some impose a cap on the amount of recoverable damages (Michigan, New Jersey and Utah) while others do not (Illinois, Maryland and Washington).

Practical difficulties created by the patchwork

The new and continuously evolving interplay between personal social media and the workplace can complicate efforts to discern the practical implications of these laws for employers. In addition, to date, no administrative enforcement action or private lawsuit has been filed that might provide examples of alleged violations of these new laws. Nonetheless, several practical implications for employers are discernible.

In the recruitment process, employers can avoid violating the new laws by limiting their searches to information that is publicly available. For some employers, however, that limitation could be detrimental to the job applicant. For example, an employer seeking to hire an employee to manage the organization's Twitter feeds might not be able to identify the applicant's personal Twitter feed without asking for the applicant's Twitter handle because the handle rarely matches the user's name. Even though Twitter feeds are publicly available, such a request might violate social media password protection laws that do not expressly except publicly available social media content from their purview. An employer might avoid this problem by asking the applicant to provide the Twitter handle for any business-related account. That request might prompt the applicant to offer the Twitter handle of the applicant's personal Twitter feed.

As US employers increasingly flock to social media to advance their organizations' business interests, they need to take these new laws into account. Employers, for example, may unwittingly permit employees to use a personal LinkedIn account to build a customer database, a personal Facebook page to develop customer relationships, or a Twitter feed to build an online following. In at least some states, the employer would not be able to demand the log-in credentials for such accounts, without risking litigation, unless the employer had documented, in advance, the employee's agreement that the account is a business account and not a personal account. Employers could avoid this issue altogether by expressly prohibiting employees from using any personal social media account to conduct company business.

The laws also have a potentially significant impact on workplace investigations. Employees commonly "rat out" their co-workers by bringing a screenshot of a co-worker's offensive or threatening social media post to the attention of a manager or the human resources department. Given the high potential for fraudulent or doctored Internet posts, testing the authenticity of the offending post and understanding its context are critical. As a result, many investigators might react to the volunteered content by asking the accused for access to his or her social media page, without considering whether the account is restricted and, therefore, the request potentially unlawful. Consequently, employers with employees in any of the twelve states with a social media password protection law should train managers and human resources professionals to proceed with caution in their investigation of suspected social media misconduct, and to consult with in-house or outside counsel before accessing content on an employee's personal social media page that is not publicly available.

Finally, employers must recognize the law in this area is evolving rapidly, demanding regular monitoring for new developments. Nineteen (19) states currently have social media password protection bills pending. In addition, existing laws already are being amended. For example, in August 2013, Illinois amended its law, originally enacted just over a year earlier, to permit employers to request or require log-in credentials for accounts used for business purposes.

Key Considerations for Any Future Legislation

Multinational employers should note the development of similar legislation in the European Union and view the United States' experience as a cautionary tale. To the extent that any such legislation is considered in the European Union, employers should be sure to express their concerns when the legislation is under consideration about whether it even is necessary as the Littler Mendelson surveys suggest that employers — at least in the US —rarely request that applicants provide the log-in credentials for their personal social media accounts. Moreover, the purpose and proportionality requirements in the national laws implementing the EU Data Protection Directive arguably establish adequate protection for applicants and employees. Under these requirements, an employer could not lawfully process an applicant's or employee's social media log-in credentials, or otherwise access the individual's personal social media account,

without a legitimate purpose for doing so that is not outweighed by the individual's fundamental rights.

Nevertheless, if new legislation must be enacted, the US experience strongly supports developing model legislation that can provide a higher degree of uniformity among the Member States than exists among the states in the US Such model legislation should include the following key elements:

1. Solely prohibit employers from requiring, as a condition of employment, that applicants or employees disclose information needed to access their own personal Internet accounts, but permit employers to search content about applicants and employees that is relevant to a legitimate business purpose and is publicly available on the Internet;
2. Exclude from coverage any account owned and operated by an employer or used by an employee to conduct the employer's business or any account used to impersonate an employer's account;
3. Include a robust investigation exception that allows employers to access information contained in an employee's personal Internet account: (1) where the employer reasonably believes that the content is relevant to an investigation of an alleged violation of the employer's policies or procedures or of any law, regulation or rule of a self-regulatory organization; or (2) where necessary to comply with the requirements of any law, regulation, or rule of a self-regulatory organization;
4. Include an exception that permits the employer to access information in an employee's personal Internet account or request log-in credentials to the account where the employer reasonably believes that the employee has transferred the employer's trade secrets or confidential business information using the account;
5. Exclude as a violation of the law any inadvertent capturing of an employee's log-in credentials, provided that the employer does not use the credentials to access the account in violation of the law; and
6. Offer immunity from negligent hiring and negligent retention claims to employers who choose to implement policies not to request or require that an applicant provide access to restricted personal Internet accounts.

REFERENCES

1. See e.g. www.dailymail.co.uk/news/article-2111059/Colleges-jobs-asking-Facebook-email-passwords-job-interviews.html; see also Philip Gordon and Lauren Woon, Re-Thinking and Rejecting Social Media "Password Protection" Legislation, available at http://privacyblog.littler.com/2012/07/articles/state-privacy-legislation/rethinking-and-rejecting-social-media-password-protection-legislation/, addressing the dubious history of these news articles in more detail
2. Littler Mendelson Executive Employer Survey Report (June 2012), available at http://www.littler.com/content/littler-mendelson-executive-employer-survey-report-2012; Littler Mendelson Executive Employer Survey Report (July 2013), available at http://www.littler.com/publication-press/press/littler-survey-reveals-employers-adjusting-economic-conditions-feeling-impac
3. The following other laws may at some point also be interpreted to prohibit this activity: California, which prohibits employers from "requesting" that an employee "Divulge any personal social media;" Illinois, which prohibits employers from "demand[ing] access in any manner to an employee's or prospective employee's account or profile;" Michigan, which prohibits and employer from "Request[ing] an employee or an applicant for employment to grant access to, allow observation of, or disclose information that allows access to or observation of the employee's or applicant's personal Internet account;" New Jersey, which prohibits employers from in "any way provid[ing] the employer access to, a personal account;" and New Mexico, which prohibits employers from "demand[ing] access in any manner to a prospective employee's account or profile on a social networking web site."
4. As noted above in footnote 3, it remains to be seen whether states with ambiguous coverage language will interpret their laws to prohibit this activity.

AUTHORS

Phillip L. Gordon, Shareholder and Chair, Privacy and Data Protection Practice Group at Littler Mendelson, Denver, Colorado, USA, and William J. Simmons, Associate, Littler Mendelson, Philadelphia, Pennsylvania, US
Emails:pgordon@littler.com
wsimmons@littler.com

Your Subscription **includes**

1. Six Reports a year
The *Privacy Laws & Business (PL&B) International* Report, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from more than 100 countries – new laws, bills, amendments, codes and how they work in practice.

2. Helpline Enquiry Service
Subscribers may telephone, fax or email us with their questions such as: contact details of Data Protection Authorities, the current status of legislation and amendments, and sources for specific issues and texts.

3. Email updates
We will keep you informed of the latest developments.

4. Index
A cumulative Country, Subject and Company index is available at www.privacylaws.com/Publications/report_index/. Subject headings include Binding Corporate Rules, data breaches, data security, encryption, enforcement, sensitive data, subject access and transborder data flows.

Electronic Option
The electronic **PDF format** of *PL&B* reports is available as soon as the report is published. This format includes click-through links from email and web addresses in the document and also links to related articles in earlier publications.

Privacy Laws & Business has clients in more than 50 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times *lists; and 10 of the Global Top 20 in the* Fortune *list.*

Privacy Laws & Business also publishes the United Kingdom Report, *a publication which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.*

Subscription Form

Subscription Packages

(VAT will be added to PDF subscriptions within the UK)

Single User Access

❑ *PL&B International* Report Subscription **£500**

❑ *UK/International* Reports Combined Subscription **£800**

Subscription Discounts

Discounts for 2-4 users or 5-25 users

Number of years: 2 (10% discount) or 3 (15%)

Go to www.privacylaws.com/subscribe

Special academic rate – 50% discount on above prices – contact the *PL&B* office

Subscription Includes:

Six new issues of each report, on-line access to back issues, special reports, and event documentation.

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Accounts Address (if different):

Postcode:

VAT Number:

❑ Purchase Order

❑ Cheque payable to: *Privacy Laws & Business*

❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

Please return completed form to:
Subscriptions Dept, Privacy Laws & Business,
2nd Floor, Monument House, 215 Marsh Road,
Pinner, Middlesex HA5 5NE, UK
Tel +44 20 8868 9200 Fax: +44 20 8868 5215
e-mail: sales@privacylaws.com 11/10

www.privacylaws.com

Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.