

2013/14 Survey

Social Media in the Workplace Around the World 3.0





About Our Survey

We are proud to present Proskauer's third annual global survey about social media use in the workplace.

As in previous years, in addition to our survey results, in collaboration with select law firms across the world, we have included a brief summary of the law from around the world, including significant recent developments.

Please note that the information provided in this survey is not intended to be, and shall not be construed to be, the provision of legal advice or an offer to provide legal services, nor does it necessarily reflect the opinions of the firm, our lawyers or our clients. No client-lawyer relationship between you and the firm is or may be created by your access to or use of this survey or any information contained in it. Proskauer Rose LLP (Proskauer) is not obligated to provide updates on the information presented herein.

© Proskauer Rose LLP. All Rights Reserved.

Social Media in the Workplace Around the World 3.0

When we published our first survey in 2011, there was a sense of novelty and even mystery about social media usage in the workplace. There was a strong perception that social media and business did not mix. The art of harnessing social media for business lacked the sophistication and prominence that it now has. Today, business use of social media is mainstream.

This shift from novel to normal in business is backed up by our survey results – 90% of businesses now use social media for business purposes.

The near ubiquitous use of social media for business has led to a maturing appreciation of workplace risks arising out of its misuse – the more that people use social media for business purposes, the greater the chances that the fine line between personal use and business use will blur.

There has been a marked increase in the number of businesses that have implemented social media policies. In addition, many businesses have introduced measures to address the specific risks arising out of social media misuse by their employees, such as bullying and harassment, misuse of confidential information and the making of disparaging comments about businesses and colleagues. All of which can cause significant reputational damage – with a tap of a keyboard, many years of careful and expensive branding and marketing can be undermined.

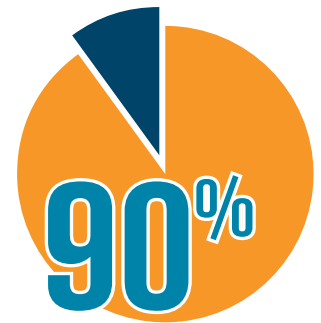
As our survey results demonstrate, these protections are necessary, due to the sharp increase in the number of businesses that have had to deal with social media misuse by employees.

However, businesses should and could be doing more to reduce the risks they face.

The importance of taking these risk-reducing actions is all the more pressing given our finding that the overwhelming majority of businesses anticipate that social media misuse is going to increase in the future.

In recognition of the need for risk-reducing actions, due to developing case law and the absence of any specific laws dealing with social media monitoring, this year's survey includes a new section summarizing best practices.

For further advice about how you can protect your business and its reputation from the risks of social media misuse, please contact the Proskauer team listed at the back of the survey.



Nearly 90% of businesses now use social media for business purposes

“Businesses should and could be doing more to reduce risk.”

Top 5 Things Employers Should Do Now:

- Annual Audits
- Make Training a Priority
- Identify Specific Risks
- Implement Clear Guidelines
- Don't Forget Ex-Employees

A Summary of Findings and Developments

We received more than 110 responses from a broad range of businesses, many with a global presence. These revealed a number of notable findings and developments.

- Nearly 90% of businesses now use social media for business purposes.
- Social media misuse in the workplace has increased. For the first time since conducting this survey, the majority of businesses have had to deal with social media misuse. Moreover, more than 70% of businesses reported having to take disciplinary action against employees for misuse (compared to 35%).
- In the last year, businesses have focused on implementing and reviewing social media policies:
 - The number of businesses with policies has increased significantly, from 60% to nearly 80%.
 - More than half of businesses have updated their policies in the last year.
- In addition to implementing policies, businesses are now taking precautions to protect against specific risks associated with misuse of social media, such as:
 - Misuse of confidential information (80%)
 - Misrepresenting the views of the business (71%)
 - Inappropriate non-business use (67%)
 - Disparaging remarks about the business or employees (64%)
 - Harassment (64%)
- Training employees reduces risks, yet, there has not been any significant increase in the number of businesses providing employees with training on appropriate use of social media.
- Only a small minority of businesses (17%) have provisions that protect them against misuse of social media by ex-employees, despite the fact some misuse (13%) involved ex-employees.
- There has been an increase in the number of businesses taking measures to stop employees from using social media at work. We found that:
 - 36% of employers actively block access to such sites, compared to 29% last year.
 - 43% of businesses permit all of their employees to access social media sites, a fall of 10% since our last survey.

110

Responses

70% of
businesses
reported
disciplinary
action against
social media
misuse in
the office

80%

of businesses
with policies
in place

The Law Around the World

Notwithstanding local differences and developments, there remains a high degree of similarity in the approaches taken in different jurisdictions on the use of social media in the workplace. As the current position develops rapidly, we have provided a synthesized summary of answers to some of the most frequently asked questions, focusing on commonality around the world as well pointing out local differences where these exist. The jurisdictions covered are: **Argentina, Brazil, Canada, China, Denmark, France, Germany, Hong Kong, India, Ireland, Italy, Japan, Spain, The Netherlands, the United Kingdom** and the **United States**.

Are Employers Permitted to Monitor Social Media Use by Employees at Work?

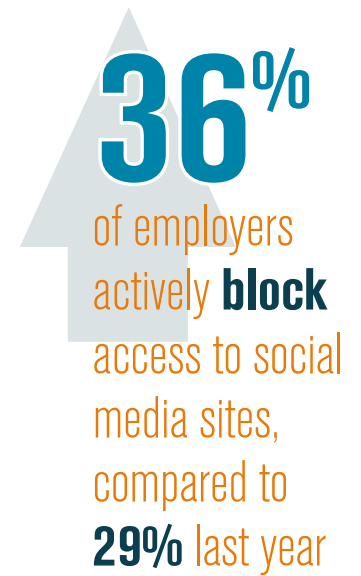
For most jurisdictions covered, the answer is yes, but with constraints on the extent to which monitoring is permissible as well as requirements that need to be satisfied to ensure the monitoring is lawful. As to monitoring social media usage on an employee's own devices (such as a smartphone), across all jurisdictions, employers do not generally have a right to carry out such surveillance.

Across all jurisdictions, factors (whether individually or collectively) relevant to the right of employers to monitor include:

- Data protection laws;
- Privacy laws;
- Rules requiring consultation with employee representative bodies; and
- Securing the consent of the individual employee.

Unsurprisingly, there are no actual laws or statutes specifically addressing the issue of monitoring social media usage, albeit that in the United States, the National Labor Relations Act plays a pivotal role in this issue.

As a result, the common approach to this issue is to apply general legal principles, especially drawing analogies from case law pertaining to other technologies (such as email). In most jurisdictions, the approach of the courts is to seek to balance, often on a case-by-case basis, an employer's right to demand that employees attend to their work with the employee's right to maintain personal privacy. Where data protection laws exist, such regulations limit the scope and methodology of collection and the eventual usage of information gathered by an employer's social media surveillance.



What Limits and Considerations Apply to Employers' Monitoring of Social Media Use by Employees at Work?

As noted, in the majority of jurisdictions the key consideration is to balance an employer's legitimate interest in protecting its business against an employee's right to privacy (and data protection considerations).

Accordingly, a best practice approach should be taken, and employers should implement the following steps if monitoring employees' use of social networking sites:

- Put in place clear, well-defined and well-communicated policies or contractual provisions concerning the appropriate use of social networking sites and the sanctions for non-compliance;
- Ideally, employees should explicitly consent to such policies in writing. In certain jurisdictions, such as **The Netherlands** and **France**, express consent will not be sufficient in and of itself to allow monitoring;
- Monitoring should go no further than is necessary to protect the employer's business interests;
- Monitoring should be conducted only by designated employees, who have been adequately trained to understand the limits on their activities;
- Personal data collected as a result of any monitoring should be stored safely, not tampered with, not disseminated more widely than is necessary nor stored longer than is necessary;
- Train management and employees in the correct use of information technology; and
- Be able to particularize and document any misuse of social media sites by employees.

Notwithstanding these general guidelines on best practices, we would note the following features that are specific to particular jurisdictions:

Argentina: Social media are considered "work tools" in Argentina, which gives employers the right to monitor the amount of time employees spend on such sites but not the right to monitor the content. To avoid creating an expectation of privacy, company policies, explicitly agreed to by employees, must clearly state the applicable rules in relation to monitoring social media usage.

Brazil: Privacy is a constitutionally guaranteed right, and as a result, any monitoring should be disclosed as a company policy in advance to employees and made subject to the express written consent of affected employees.

Canada: Surveillance of employees' use of social networking sites by the employer is permitted; however, such monitoring must be reasonable and not rise to the level of an invasion of privacy. Under the common law, the tort of invasion of privacy is generally the main source of employee privacy rights. Although this cause of action has had a mixed reception in Canada, the Court of Appeal in Ontario recently recognized a common law right of action for invasion of privacy. The tort, specifically referred to as the tort of "Intrusion Upon Seclusion", has been described as follows: "*[o]ne who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person.*" There are three key elements that form the basis of the cause of action: (i) the conduct in question must be intentional, which includes recklessness; (ii) there must be an invasion, without lawful justification, into an

individual's private affairs or concerns; and (iii) the invasion must be highly offensive, causing distress, humiliation, or anguish to the reasonable person. While it is still too early to assess the risks posed by Ontario's new tort of intrusion upon seclusion in the employment context and specifically upon the monitoring of social media, recent jurisprudence suggests that there is an appetite to limit the types of cases in which it can be applied.

China: Employers should only monitor the use by employees and deal with the data collected in a way that complies with the interest and moral standards of the society. In addition, a policy involving monitoring social media use would be regarded as a material matter that affects the interest of employees. As a result, an employer should consult the employee representatives committee and labor union when establishing, modifying and implementing such a policy, and allow the employees to have a chance to review and comment on any policy prior to its implementation. Once the policy is implemented, an employer does not have to consult employees or their representatives about implementing the policy on a case-by-case basis.

France: Before an employer can monitor employees' use of social media, it must inform and consult its works council, and the affected employees must be informed that monitoring is to take place and its purposes. If these requirements are not met, the information gathered by the monitoring process cannot be used to discipline an employee. In addition, the French data protection agency must be informed that monitoring is taking place if (as is usually the case) it will result in storing, recording or otherwise processing data about identifiable individuals. Finally, where an employer wants to implement a policy on the use of social media which contains disciplinary sanctions for non-compliance, the policy must be regarded as an addendum to the internal rules of the company, and its introduction will require a specific procedure (which includes consultation and filing of the policy before the French labor administration).

Germany: Although works councils need not be informed about monitoring in individual cases (even though in some cases this may be advisable), for any monitoring that can impact an entire business, such as the introduction of monitoring policies, works council involvement will be required.

Hong Kong: The local data protection agency has issued guidelines for reconciling employer monitoring with personal data protection at work. These provide that prior to deciding whether to embark upon employee monitoring, employers should conduct due diligence by undertaking a systematic assessment process to determine whether employee monitoring is the best option given the risks and activities the employer seeks to manage. The guidelines also recommend the employers should consult, and take into consideration, the views expressed by employees in determining the parameters to any workplace monitoring, which would extend to the monitoring of social media use. If an employer anticipates that personal data will be collected in the process of monitoring, the employer should expressly inform its employees of the monitoring activities beforehand. This is usually done by a written Personal Information Collection Statement which sets out, in advance of any monitoring:

- The purpose for which the personal data collected will be used;
- Whether it is obligatory or mandatory to supply the data;
- The classes of persons to whom the personal data will be transferred; and
- The rights of the employees to request access to and to correct their personal data.

India: While there are no specific legal restrictions against monitoring social media use, most employers, as a matter of good practice, inform employees (through the code of conduct/ employment handbook/manual) about their right and ability to monitor such usage. In a recent development, in December 2013, India enacted a new law prohibiting sexual harassment of women in the workplace. A provision prohibiting sexual harassment was also introduced in the Indian Penal Code. Under the new laws, sexual harassment is very broadly defined and could also include showing pornography whether directly or by implication, via use of social media, in the workplace. Given this is new law, it remains to be seen how employers in India will respond to it, and whether it will lead to changes in their social media policies and practices.

Ireland: Any limitation on the employee's right to privacy should be proportionate to the likely damage to the employer's legitimate business interests. The government agency responsible for data privacy in Ireland has issued guidance notes on monitoring staff in the workplace. Employers are advised to have in place an acceptable usage policy reflecting the balance between the employer's legitimate interests and an employee's right to privacy. The principles of data protection require transparency, fair and lawful possessing of data and the need to ensure that any encroachment on an employee's privacy is fair and proportionate. Importantly, staff must be informed of the existence of the surveillance.

Italy: Employers are generally not permitted to monitor the content of social media. However, an employer in Italy may prohibit the use of social networking sites during work hours and is also permitted to monitor social media sites to determine whether an employee has used them in breach of any policies (and impose sanctions against an employee for breach of any policies). Such monitoring must be limited to ascertaining whether or not the employee used the social networking sites and may not involve any review of the data and information posted or viewed by the employee. Furthermore, this limited monitoring is only permissible if an employee is given prior notification (as a part of a company policy) about:

- How such monitoring is to be executed;
- Its purposes;
- How long personal data will be held by the company; and
- The safeguards in place to prevent the misuse of personal data.

In addition, any prohibition on social networking at work must be part of a policy which clearly sets out the extent to which use of social networking is permitted and the steps the company will take to monitor compliance with the policy. Any such policies must also be accepted by employee representative bodies (usually the works council or the labor office). These requirements cannot be circumvented or excluded by obtaining the individual consent of employees to monitor social media use—such consent would not be deemed valid under Italian law.

Japan: Monitoring must not infringe on employees' privacy nor violate the parameters outlined in the Personal Information Privacy Act (PIPA) which delineates the appropriate collection of personal data. Best practices dictate that an employer's right to monitor employees' usage of social media sites on company devices without prior notice or consent should be clearly stipulated in employment contracts or company regulations.

Spain: Employers are permitted to monitor the time spent by employees on social media while they are at work (provided that employees have previously been informed that such monitoring will take place, ideally through a policy or a code of conduct), but in most circumstances employers may not monitor the content of a social networking site (such as an employee's postings) without the consent of the employee or reports from other individuals who have legitimate access to the content.

The Netherlands: Where a company has a works council, the works council must be consulted about any policy on social networking that the company wishes to implement. In addition, the Dutch data protection authority should be notified about any monitoring. In terms of guidelines, the Dutch data protection authority recently released a checklist with do's and don'ts regarding the use of social media by employees and monitoring by employers, the most important of which were explicit recommendations that: employers are only allowed to check activities of employees on social media when there is a legitimate reason and a necessity to do so; and employees need to be informed about the possible screening of their social media activities, for example via internal guidelines.

United Kingdom: The government agency responsible for data privacy has issued guidelines about appropriate monitoring in the workplace, which should be complied with. Amongst other things, these state that any monitoring needs to be proportionate, which broadly means that the reason for monitoring has to be sufficient to justify the level of intrusion into an employee's private life. Businesses should carry out an impact assessment of any monitoring in order to determine whether it is proportionate in the circumstances.

United States: Broadly, any monitoring of social media use (and related policies) must account for the rights of workers to engage in certain collective activities, known as protected concerted activities (such as organizing co-workers, complaints about working conditions, on-the-job protests, picketing, and strikes) under section 7 of the National Labor Relations Act (the "NLRA") and the prohibition against employers interfering with or restraining employees against exercising such rights (under section 8 of the NLRA). In particular, employers must not engage in monitoring that has the effect of explicitly or implicitly restricting employees' rights to engage in activities covered by section 7 of the NLRA or enforce their rights in connection with such activities. As such, policies and practices should clearly articulate the legitimate business interests sought to be protected or achieved through the policy, and the restrictions should be narrowly tailored to serve those legitimate interests. Though disclaimers are not required, and though they do not, in and of themselves, provide an absolute defense, the inclusion of clear and express language that employees can easily understand, disclaiming any intention to restrict employee rights in respect of section 7 activities may also be helpful to defeat claims that employees may reasonably interpret the policy as restricting their rights.

Is an Employer Allowed to Prohibit Use of Social Media Sites During Work: (i) On Equipment Provided By Employers; and (ii) On an Employee's Own Devices (e.g., Mobile Phones)?

In nearly all the jurisdictions, an employer is permitted to prohibit the use of social media sites during work, both on equipment provided by the employer and on the employee's own devices. However, the prohibition against use of social media sites on an employee's own devices would

not give the employer the right to monitor such devices (which would infringe the employee's right to privacy in many jurisdictions); rather, the prohibition would be an incident of the employer's general right to require employees to devote their working hours to their work.

*One exception to this is in the **United States**, where any prohibition against the use of sites, even on equipment provided by employers, must avoid infringing the rights of employees to engage in protected concerted activities under section 7 of the NLRA.*

Even though most jurisdictions surveyed provide the employer with adequate legal foundations to justify the prohibition of access to social media during work, it is still recommended that such a practice is communicated as part of an official company policy and be supported by cogent business reasons, such as promoting the work productivity of employees (**The Netherlands**) or ensuring employees full availability during working hours (**Argentina**). Additionally, employers should be cautious about the extent to which they impose restrictions on the use of personal devices, as such restrictions could also infringe employees' rights to communicate freely (**Spain**) or be regarded as an unauthorized "interference" on personal devices (**Argentina**).

Is an Employer Allowed to Block Access to Social Media Sites During Work: (i) On Equipment Provided By Employers; and (ii) On an Employee's Own Devices (e.g., Mobile Phones)?

As with the prohibition of use discussed above, in all the jurisdictions surveyed, an employer is permitted to block access to social media sites on employer-provided equipment. Indeed, respondents from many countries indicated that not only is this method legal, but that it is a common practice among employers. A few potential pitfalls are still worth noting, such as the rules in place in **Argentina** and **Japan**, which allow policies banning use of social media but prohibit actual interference with employees' devices.

To What Extent Is it Permissible to Refer to Social Media Sites When: (i) Taking Disciplinary Action Against an Employee; and (ii) Making Decisions about Recruitment and Selection?

In most jurisdictions, it is permissible to refer to social networking sites, both when taking disciplinary action against an employee and when making decisions about recruitment and selection. There are, however, some exceptions.

In **France**, the law is unsettled on the point of exactly when and how information found on social networking sites can be used by an employer for disciplinary measures. Indeed, case law is divided with respect to the ability of employers to sanction employees who have posted negative comments.

In **Italy**, it is not permissible to refer to social networking sites to make decisions about recruitment and selection of candidates, broadly because referring to social media sites in such a context would be an infringement of an individual's right to privacy. Similarly, in **Canada**, using social media in the recruitment and selection process risks violating privacy laws. Canadian privacy regulatory authorities have issued guidelines and decisions providing advice to organizations on how much information can or should be collected through social media when performing a background check. These suggest it may be difficult for businesses to comply with privacy laws if they collect information from social media sites in the recruitment and selection process.

In the **United States**, under the NLRA as currently interpreted, an employer may generally not take action against an employee who posts items critical of the employer's employment practices, subject to the posts being joined in by co-employees, or being for the purpose of urging, preparing for, or carrying out concerted complaints or actions. An employer also may not discriminate against an employee or applicant based on posts which indicate previous support of or involvement in union or protected concerted activities.

Similarly, with regard to recruiting, the legal landscape is in flux. For this reason, various French headhunters have adopted a code of conduct stressing that applicants' selection should only rely on their professional skills and exclude all elements pertaining to privacy; as a consequence, many companies have undertaken to avoid looking at social networking sites when recruiting. **Germany** limits consultation to business-oriented social media, whereas **The Netherlands** and **Spain** allow any publicly accessible information to be used.

All jurisdictions warn of the great risk employers run in using such information, as it opens the door to discrimination lawsuits claiming that decisions were based on improper considerations. In any event, and notwithstanding the general ability in many jurisdictions to refer to social networking sites in relation to disciplinary action, recruitment and selection, the following should be kept in mind (which are common to all jurisdictions):

- An employer would be well-advised to consider carefully the evidentiary weight to be given to information obtained from a social media site;
- The information posted may be inaccurate, out-of-date, not intended to be taken at face value, or even posted by someone other than the person who is the subject of the inquiries;
- Relying on information contained in social media sites creates a risk of discrimination, either because someone is treated less favorably by reason of a protected characteristic, or a condition is imposed that has a disparate impact on a particular group; and
- Any use of social media sites when making employment decisions should comply with data privacy requirements (including in relation to the secure storage and deletion of information after it is no longer needed) and any internal policies about monitoring of such sites.

In relation to these issues, it is worth noting that The Netherlands Association for Human Resources Management and Development of Organizations has developed a code of conduct, which, although drafted specifically for that country, contains suggestions that would not be out of place in other jurisdictions. The code of conduct provides, among other things, that information about a job applicant that has been obtained from social networking sites:

- Should be discussed with such job applicant before relying upon it;
- Should be treated confidentially; and
- Should be deleted within four weeks after the job application if the applicant is not hired (unless the applicant consents to such information being kept for a maximum period of one year).

In addition, it is recommended that applicants be informed at the start of any application process that information about them that is online, including on social media sites, will be used as part of the selection process.

To What Extent Can Employers Limit the Use of Social Media Sites by Their Employees Outside of Work?

In all jurisdictions, an employer has no right to prohibit the use of social media per se. However, employees are not entitled to use social media to engage in actions that would otherwise be impermissible, such as misusing confidential information, infringing intellectual property rights, harassing another employee, or otherwise breaching the duties they owe to their employers. It would, therefore, be prudent for any policy on social networking to make clear that employees can be held responsible (and can be disciplined) for work-related misconduct that they engage in on a social networking site, even on their own time (albeit that in the **United States**, although such limitations are possible, any such policies have to be carefully worded to ensure they do not infringe the rights of employees under section 7 of the NLRA).

Because employers do not have the legal tools to proactively prevent their employees from expressing themselves on social media outside of work, any corrective action necessarily comes after the offensive information has been posted.

To What Extent Do Companies Have Social Networking Policies in Place?

The general consensus is that broad information technology and communications policies are almost ubiquitous. In addition, as our survey shows, the number of employers who now have dedicated social media policies has increased significantly, to nearly 80%, with the figures suggesting that most of those who have introduced new policies have them covering usage both at work and outside of work.

Recent Developments On Social Media Use and Misuse

In this section, we focus on recent decisions from a number of jurisdictions that are illustrative of the growing body of case law related to social media use in the workplace. As the cases illustrate, this is an issue where courts have to grapple with the balance between an employee's rights to free speech and privacy and an employer's rights to protect its business interests and take disciplinary action against employees who harm such interests.

Argentina

There have been a number of decisions in the last year which show the difficulty of relying on social media to justify a termination.

In the case of *B.M.L. v. SAV S.A.* (Labor Chamber, Room II) – December 27, 2012, The Labor Chamber, an employee was dismissed amidst allegations of having posted pictures on a social media site that damaged the employer's brand. The employer alleged that the dismissal was justified and lawful because of the moral and economic damage caused by the pictures posted by the employee. The court found in favor of the employee, holding that the pictures did not constitute objective evidence of the alleged damage suffered.

In *M.L.A. v. SAV S.A.* (Labor Chamber, Room II) – June 11, 2013, an employee was dismissed for drinking alcohol at work. The employer's decision to terminate relied upon evidence contained in pictures posted on Facebook. The Labor Chamber ruled in favor of the employee, holding that mere pictures of the employee drinking did not justify the termination because the employer was not able to show from the picture that the employee's actions caused it any harm.

In *B.P.I. v. Empresa Distribuidora y Comercializadora Norte S.A.* (Labor Chamber, Room II) – October 15, 2013, an employee was terminated for cause based on evidence from LinkedIn which showed that he had spent part of his working time conducting business for his own benefit and not his employer's. In this case, and in contrast to the other cases referred to, the Labor Chamber found the termination to be lawful. On the surface, it is difficult to reconcile this decision with others – which of itself highlights the perils of relying upon social media to make employment-related decisions.

Canada

The case of *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62, November 13 2013, dealt with the balance between freedom of expression and the rights to privacy.

During a lawful strike at the Palace Casino at the West Edmonton Mall in Alberta (the "Casino"), which lasted 305 days, the Union and the striking employees video-taped and photographed visitors to the Casino crossing the picket-line to access the Casino. In the picketing area, the Union posted signs stating that the images of persons crossing the picket-line might be placed on a website. Several individuals filed complaints with the Alberta Information and Privacy Commissioner. The Adjudicator concluded that the Union's use and disclosure of the information was not authorized by the Personal Information Protection Act (the "PIPA"). The constitutional validity of the relevant provisions of the PIPA was thereafter contested before the higher courts. The Supreme Court of Canada was ultimately called upon to determine the constitutional validity of the provisions of the PIPA.

Before the Supreme Court, the main issue was whether the PIPA achieves a constitutionally acceptable balance between the interests of individuals in controlling the use and disclosure of their personal information and the Union's freedom of expression. The Supreme Court found that the Union's freedom of expression guaranteed under the Canadian Charter of Rights and Freedoms was violated, and that this violation was not justified or justifiable in a free and democratic society. In reaching its decision, the Supreme Court referred in particular to the following factors: no intimate details of the lifestyle or personal choices of the individuals were revealed; taking pictures of individuals in a public place was less likely to infringe upon the individuals' privacy than pictures taken in private. For these reasons, the Court struck down the provisions of the PIPA. However, the declaration of invalidity of the PIPA has been suspended for a period of twelve (12) months in order to give the legislator the opportunity to make the necessary legislative changes to the PIPA.

France

In France, the issue of whether comments made on Facebook are public or private was considered by the French Supreme Court (Cass. 1ère civ., 10 avril 2013, n° 11-19.530, FS-P+B+I). In this case, an ex-employee made insulting comments about his former employer. For the first time, the Supreme Court ruled on the status of comments made by an employee on Facebook. The question arose because public insults are subject to more severe sanctions than private insults. In this case, the Supreme Court held that the insults were private. This was on the basis that the ex-employee had configured his Facebook's profile so that the comments were accessible only to persons authorized by him and because these persons were very limited (it appears that there were only 14 people).

As a result, the issue of whether a comment on social media is deemed public or private will depend on the privacy settings that are applied to the relevant account. The more accessible a comment, the more likely it will be deemed public. This contrasts to decisions in other jurisdictions, such as the UK, where it has been held that even where social media profiles are set to private, there can generally be no expectation of privacy, and the posts will be deemed to be public.

In a slightly more unusual case, a recent appeal court decision ruled that an employee could rely on remarks made on Facebook for her benefit (CA Poitiers, 16 janvier 2013). In this case, the individual filed claim to obtain recognition that she had been an employee (which was being denied). In support of her claim, the employee relied upon material posted on Facebook by her employer, which made many references to the company having "dismissed" her. The court accepted this as evidence in support of individual having employee status.

Japan

In There have been two, recent high-profile recent incidents of social media misuse by employees.

In the spring and summer of 2013, controversy arose in Japan following numerous instances of civil servants anonymously posting slanderous comments on various social media platforms. By using the information from these social media platforms as clues, the identities of the perpetrators were discovered. Since these civil servants are required to be neutral and fair in the conduct of their public duties, they received very strong criticism from the mass media for the comments they posted. At the time the controversy arose, no rules or regulations were in place regarding the use of social media by civil servants. As a result, soon after the controversy broke in June 2013, guidelines were quickly issued by the government to prevent further instances of social media misuse.

Separately, and also in the summer of 2013, a spate of employees employed by convenience stores and other shops handling food products, started posting photos of themselves mishandling ingredients and other food-related items on various social media platforms. As a result, irate consumers brought claims and complaints against these convenience and food stores, citing a lack of hygiene and sanitation standards. Eventually, the convenience and food stores had no choice but to make arrangements for exchanges, refunds and in some particularly dire cases, store closures. One consequence of this conduct was that, although it is lawful to discipline and in some cases terminate employee for such misconduct, it is generally considered to be very difficult to seek damages from employees to compensate for reputational damage caused by their misconduct. However, in the cases of employees who posted the pictures, damages claims are easier to formulate because the damages were able to be quantified by reference to the specific exchanges, refunds and store closures caused by the social media abuse by employees

The Netherlands

The data protection authority (*College bescherming persoonsgegevens*) received a complaint from an employee because his employer had required him to place his personal information on LinkedIn. Moreover, when appraising employees, the employer gave credit to those who had LinkedIn profiles and more credit to those who regularly updated their profiles. The complaint was upheld, with the authority explicitly stating that the employer cannot require employees to place personal information on social media websites.

The authority also announced that it has received over 900 complaints in respect of privacy issues relating to the processing of personal data in the light of employment relationships – clear demonstration that the protection of the privacy of employees remains a central policy concern both for employees and the authority.

United States

In the last year, there have probably been hundreds of unfair labor practice charges filed raising employer discrimination or misconduct about the enforcement of, and many times the mere maintenance of, social media rules. The principal theories underlying nearly all of these charges have been either that:

- The social media rule directly interfered with employee rights to engage in protected activity under the NLRA; or
- The rule could be reasonably read to forbid, and thereby would “chill”, protected employee activity under the NLRA.

Because of this, many employers are reviewing their social media policies in order to narrowly tailor them to avoid such interference or chilling effect. Generally speaking, these cases tend not to be litigated. Consequently, as a practical matter, if the General Counsel of the National Labor Relations Board (the “NLRB”) issues a complaint, in the great majority of cases, the parties settle and adopt the General Counsel’s formulation of what the particular social media policy provision should say.

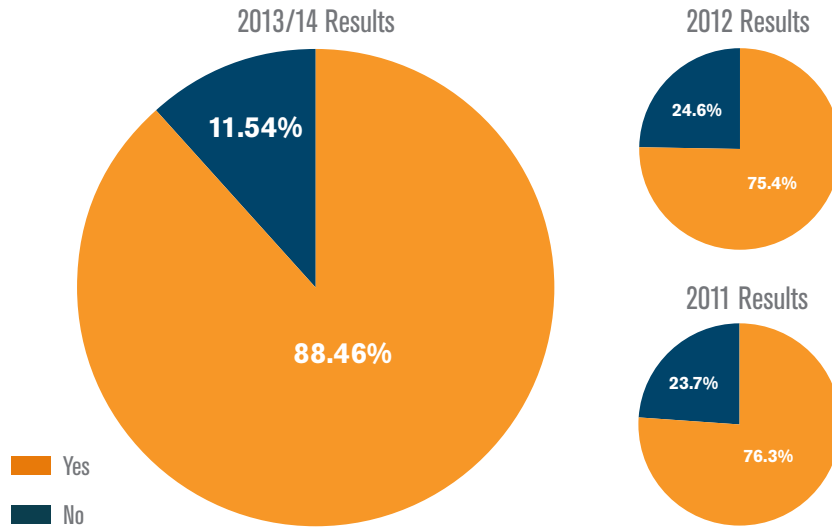
Another practical problem for employers is that there are nearly 30 NLRB regions which, in the vast majority of cases, investigate and decide whether to issue a complaint on an unfair labor practice charge, with only general guidance from NLRB headquarters. This has resulted in some national employers being hauled into cases in multiple regions, only to have one region find one social media provision unlawful, and another find a different one unlawful. In order to short-circuit this redundant process and bring some closure to the issues, some employers have sought to involve NLRB headquarters in their cases in the hopes of obtaining a “global” review and settlement on all provisions deemed unlawful.

Finally, the NLRB remains committed to prosecuting these cases, although the new General Counsel has said he plans to focus more on clearly unlawful social media provisions that actually interfere with (by, e.g., forbidding) protected conduct, rather than going after (at least as vigorously) those that may be read to “chill” such conduct. Of course, this policy could be changed and in any event is not intended to end of targeting “chilling” rules, either.

The Survey Results in Full

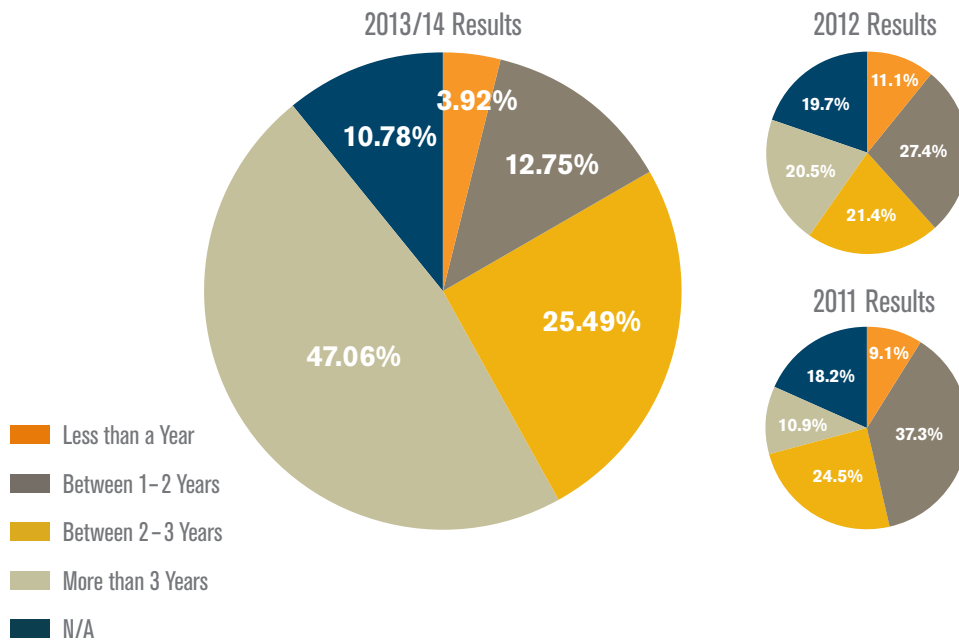
Question 1:

Does your business use social media (e.g., LinkedIn, Facebook) for business purposes?



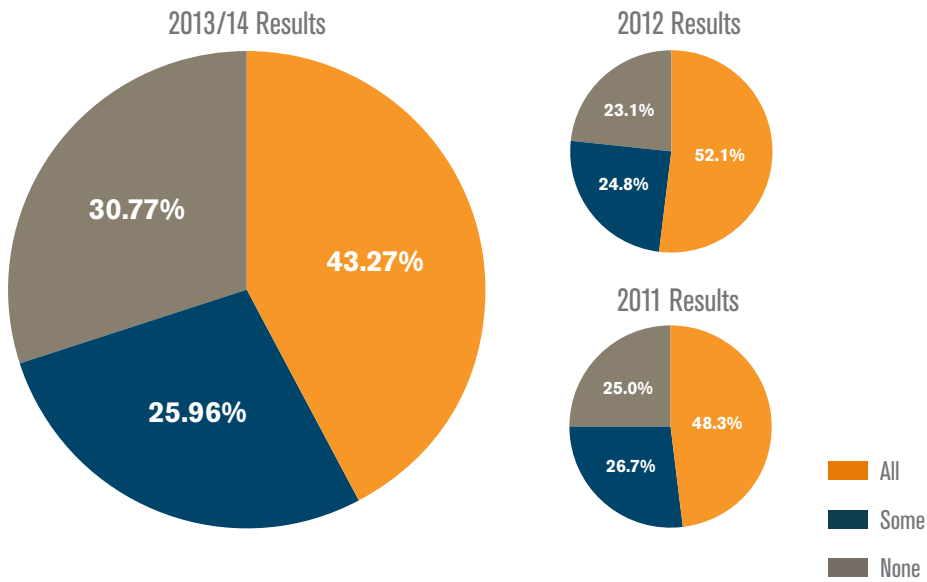
Question 2:

If your business uses social media for business purposes, how long have you used them?



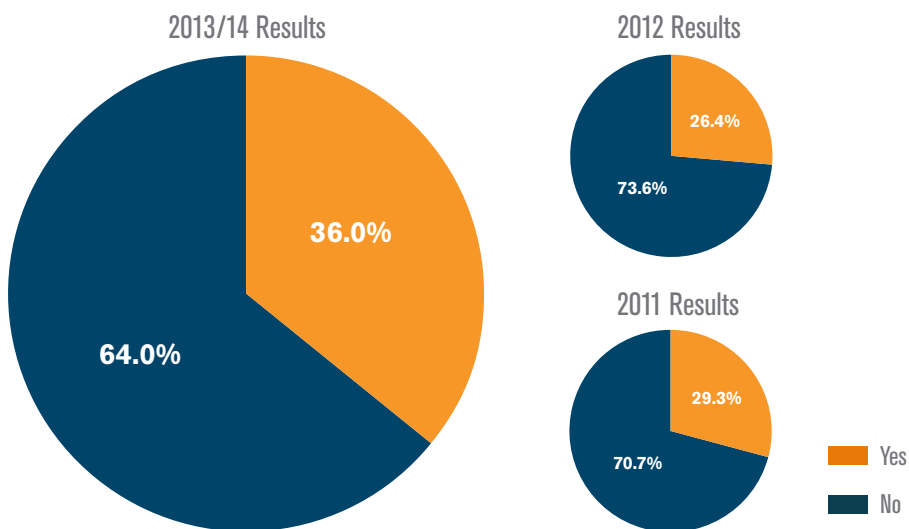
Question 3:

Are all, some, or no employees permitted to access social media sites at work for non-business use?



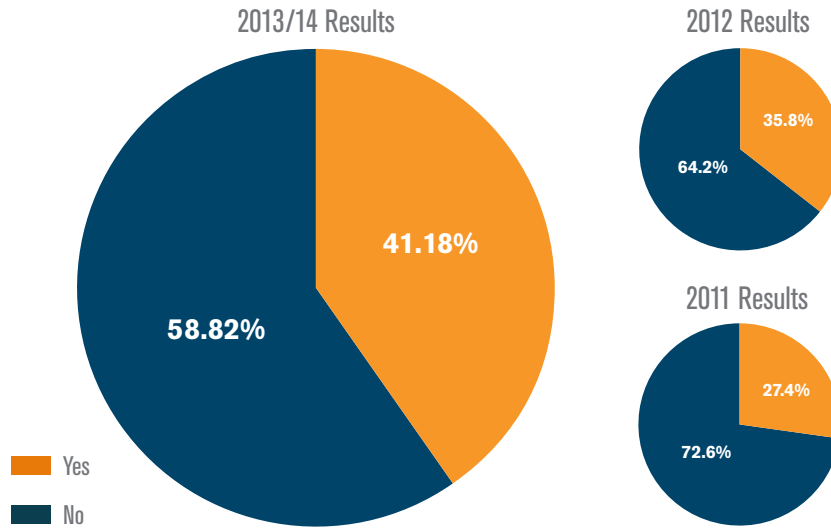
Question 4:

Do you actively block access to social media sites at work?



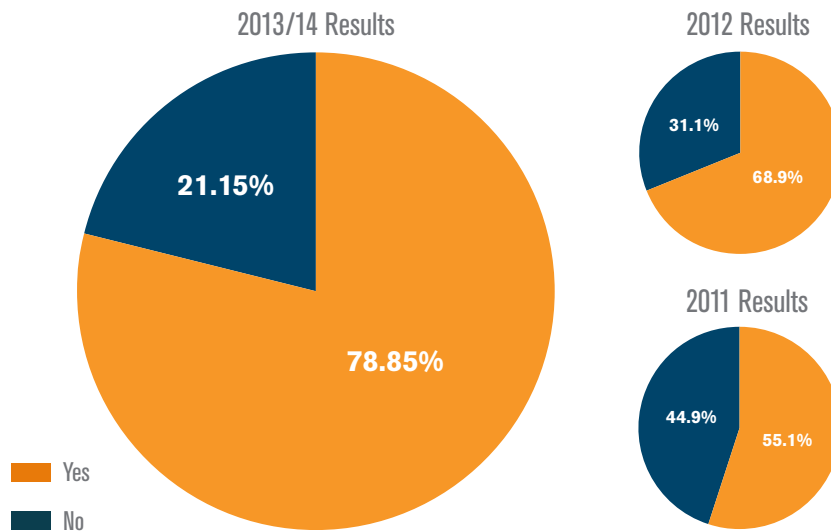
Question 5:

Do you monitor the use of social media sites at work?



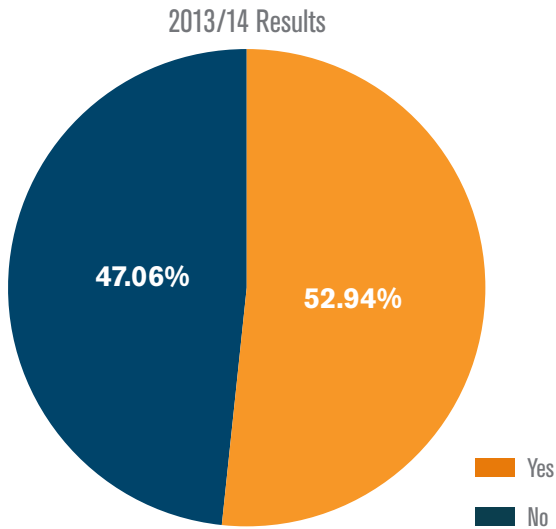
Question 6:

Do you have any policies in place in relation to social media?



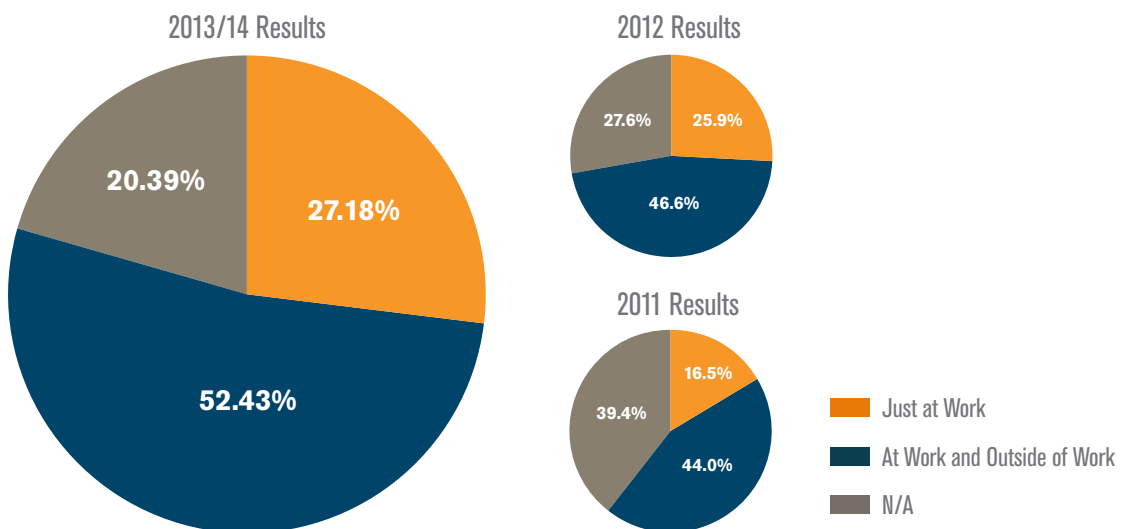
Question 7:

Has your business updated your social media policies in the past year to help manage misuse risk?



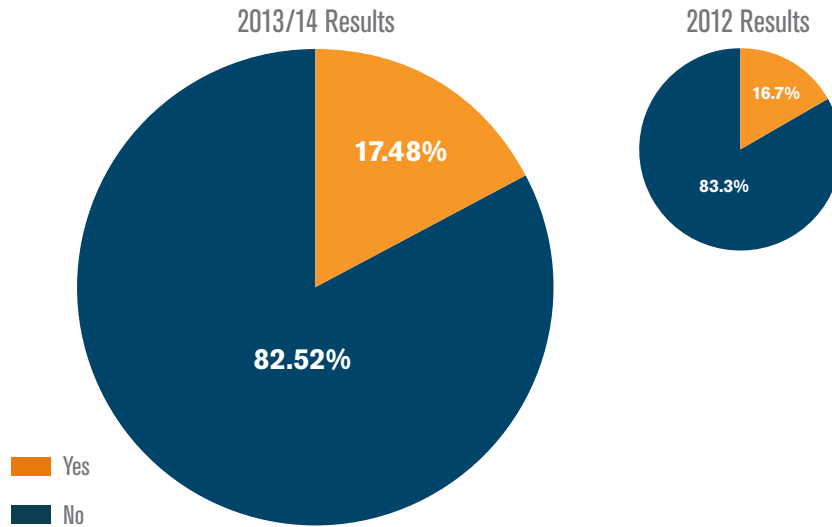
Question 8:

If you have policies in place in relation to social media, do they cover both use at work and outside of work?



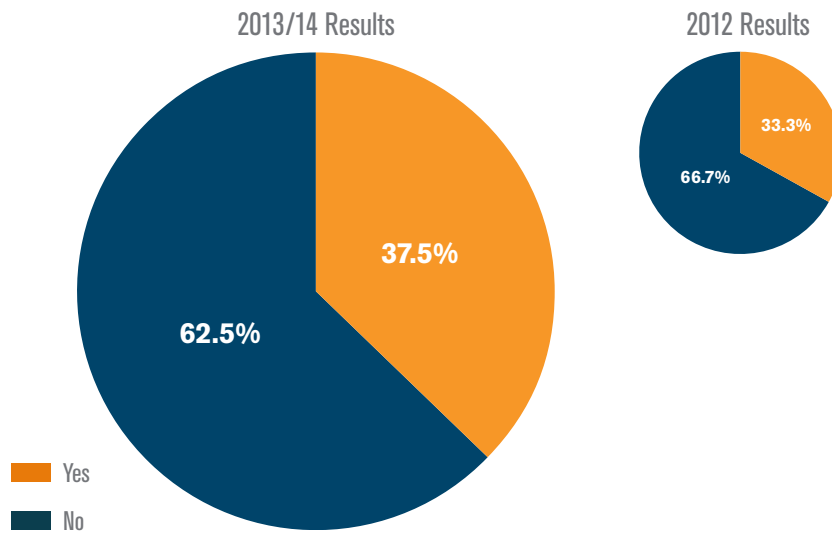
Question 9:

Do your termination provisions contain express provisions protecting against misuse of social media by former employees?



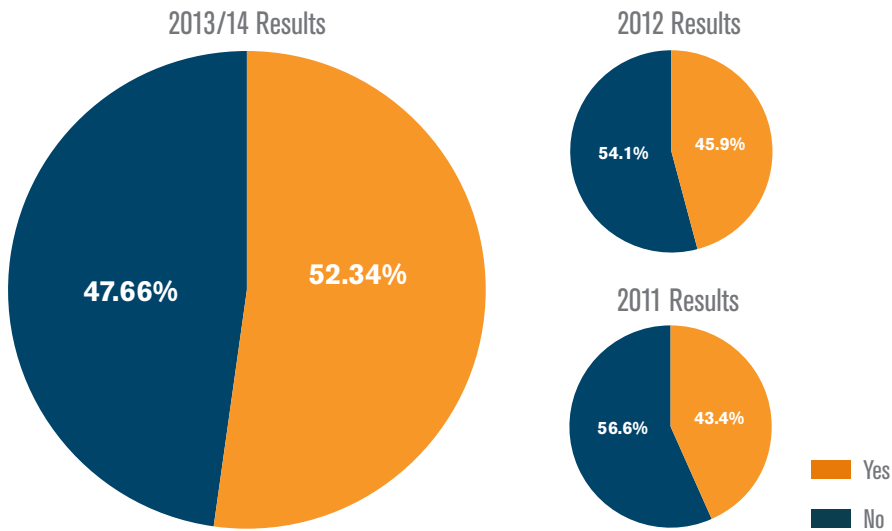
Question 10:

Do you provide employees with training on appropriate use of social media?



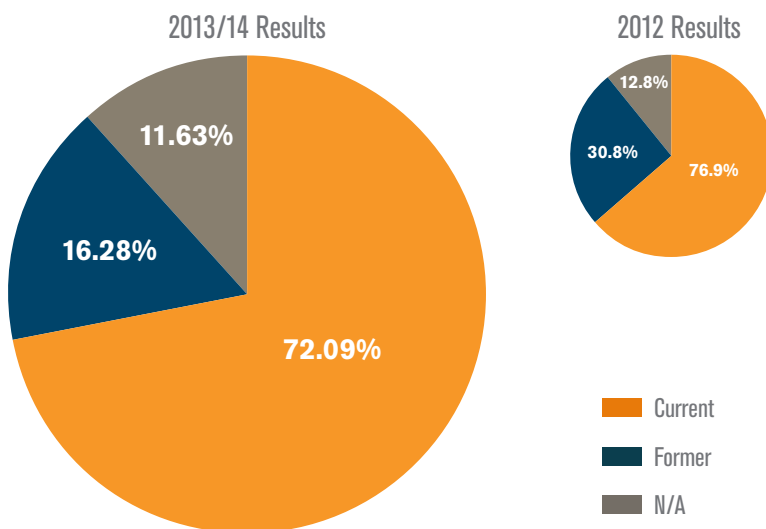
Question 11:

Is misuse of social media an issue your business has ever had to deal with?



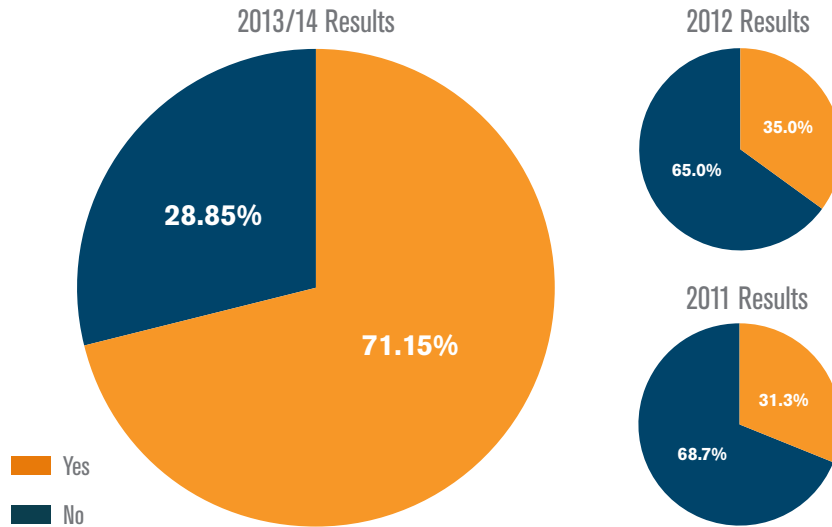
Question 12:

Was the misuse of social media an issue caused by current employees or former employees?



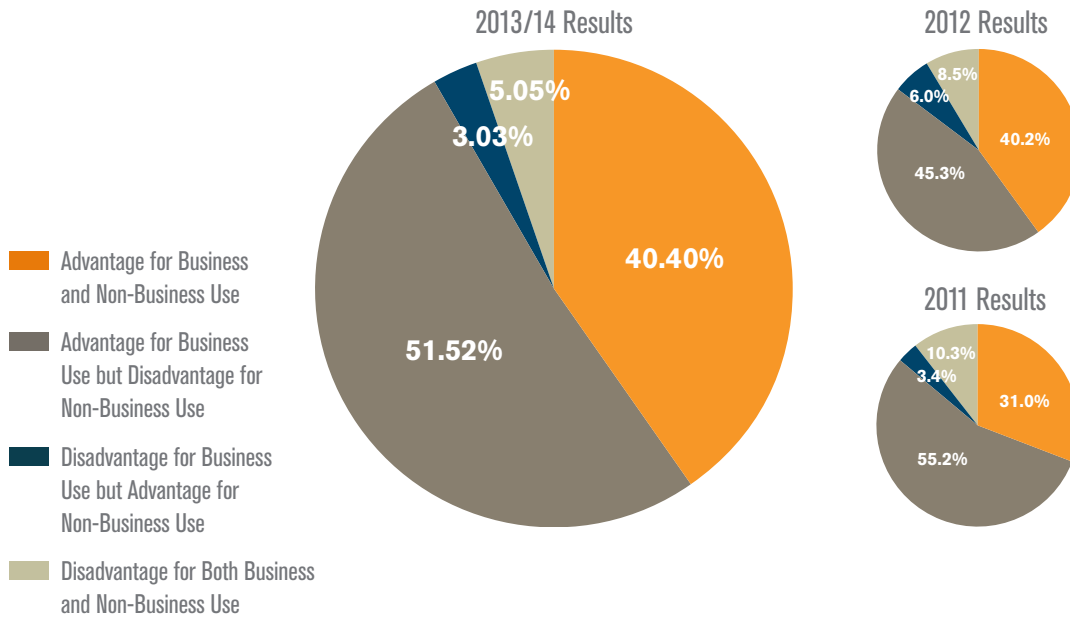
Question 13:

Has your business ever had to take disciplinary action against an employee in relation to misuse of social media?



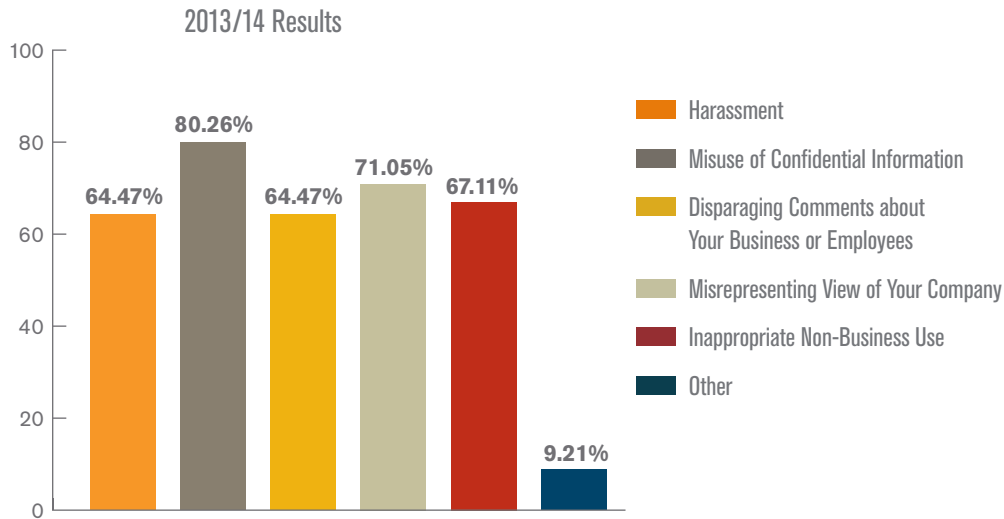
Question 14:

Do you think it is an advantage or disadvantage to your business to allow employees access to social media sites while at work for (i) business use and (ii) non-business use?



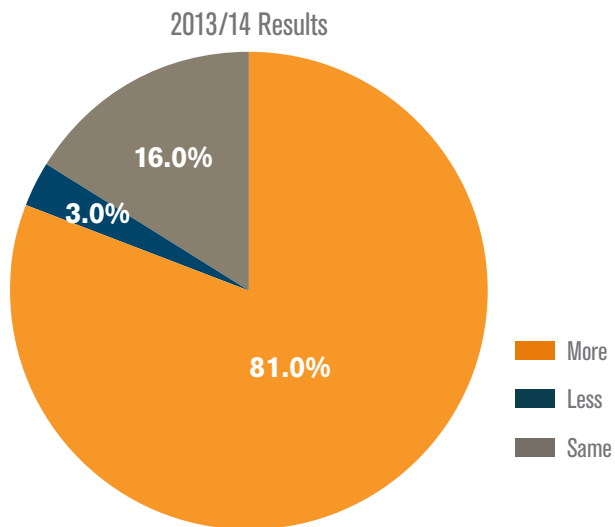
Question 15:

Has your company taken any precautions associated with protecting itself against the risk of having social media in the workplace?



Question 16:

Do you foresee the misuse of social media becoming more or less of an issue in the future?



Question 17:

Please use this space as an opportunity to share any additional thoughts relating to social media in the workplace and your employees.

"Building Trust and a culture of Open communication will ensure use of social media is driven through self responsibility and accountability".

"We allow LinkedIn but not Facebook access. Facebook is blocked. LinkedIn for business use only".

"As we have a unionized work force, though are a white collar employer, our social media policy does not prohibit comments about the employer (per NLRB rules)...".

"While we generally allow non-business-related use of social media during work hours, we do allow specific departments to adopt more restrictive rules. The areas that have done so have done so for safety reasons, and only allow access during breaktime in designated break areas or away from the employee's work areas".

"Blocking personal use of social media lowers the number of job applicants, so it's seen as a must-have item for new employees".

"Our company is in the social media business. Our employees must understand social media more so than our clients. To that end, we encourage the use of all social media channels. Our guidelines comply with the ever changing mandates set forth by the NLRB".

Best Practices: Our Top 5 Tips

1. Annual Audits: The law around the world is developing rapidly in this area. We recommend that businesses, especially global ones, carry out annual audits to ensure that their practices and policies comply with the developing legal requirements.

2. Make Training a Priority: Although specific social media policies have become the norm, not many businesses provide training to employees about the do's and don'ts of social media use. Such training reduces the risk of misuse.

3. Identify Specific Risks: Any training (as well as policies) should expressly address the specific risks that our survey shows are prevalent as a result of social media use, such as misuse of confidential information, misrepresenting the views of the business, inappropriate non-business use, disparaging remarks about the business or employees, and harassment. In parallel with this, we also recommend that policies dealing with these matters should expressly refer to social media. For example, policies dealing with confidential information should explicitly prohibit the misuse of confidential information on social media.

4. Implement Clear Guidelines: The more a business relies upon social media for business purposes, the more likely it will be that the boundary between the work and the personal use will become blurred. For those individuals who are involved in using social media for work purposes, implement specific guidelines to keep the boundary as clear as possible.

5. Don't Forget Ex-employees: Relatively few businesses have explicit provisions preventing the misuse of social media by ex-employees, despite the problems that departing employees can create – especially those with an axe to grind. We strongly recommend implementing such provisions.

Law Firm Participants

We are grateful to the following lawyers and firms who have worked with us on the summaries for each of these jurisdictions:

Argentina: Enrique M. Stile, Marval, O'Farrell & Mairal, (www.marval.com.ar)

Brazil: Dario Rabey, Souza, Cescon, Barriau & Flesch Advogados (www.scbf.com.br)

Canada: Danny Kaufer and Alexandre Buswell, Borden Ladner Gervais (www.blg.com)

China: Ying Li and Lijuan Hou, Proskauer (www.proskauer.com)

Denmark: Majken Korsgård Petersen, Danders & More (www.dandersmore.com)

England: Daniel Ornstein and Peta-Anne Barrow, Proskauer (www.proskauer.com)

France: Yasmine Tarasewicz and Cécile Martin, Proskauer (www.proskauer.com)

Germany: Thomas Winzer, Gleiss Lutz (www.gleisslutz.com)

Hong Kong: Jeremy Leifer, Proskauer (www.proskauer.com)

India: Vikram Shroff, Nishith Desai Associates (www.nishithdesai.com)

Ireland: Melanie Crowley, Mason Hayes & Curran (www.mhc.ie)

Italy: Annalisa Reale, Chiomenti Studio Legale (www.chiomenti.net)

Japan: Nobuhito Sawasaki, Kazutoshi Kakuyama and Takashi Nakazaki, Anderson Mori & Tomotsune (www.amt-law.com)

Spain: Juan Bonilla, Cuatrecasas, Gonçalves Pereira (www.cuatrecasas.com)

The Netherlands: Astrid Helstone, Stibbe, (www.stibbe.com)

United States: Erika Collins, Betsy Plevan, Ronald Meisburg and Katharine Parker, Proskauer (www.proskauer.com)

About Proskauer's International Labor & Employment Law Group

Our International Labor & Employment Law Group has decades of experience working with global companies on international and cross-border workplace issues. We have lawyers in our offices across the United States, London, Paris, Hong Kong and Beijing as well as close cooperative relationships with leading labor and employment practices around the globe. These resources enable us to provide clients with a seamless "one-stop shop" on international labor and employment matters, wherever they arise.

Through our wealth of collective know-how and experience, we have developed a deep understanding of the different cultural and legal approaches to labor and employment law throughout world and a finely-tuned sensitivity to the nuances and unique workplace issues that arise in different jurisdictions. Our knowledge extends to a wide variety of areas including restructuring, employee benefits, mergers and acquisitions, employee investigations and cross-border litigation. We deliver

clear direct and practical advice and pride ourselves on collaborating with our clients to find innovative solutions and workarounds when these are needed.

Chambers Europe praises our "renowned" team for its "vast expertise" and notes "Peers are unanimous in their admiration for the 'exceptional'" group co-head Yasmine Tarasewicz. Co-head Betsy Plevan, ranked in the first-tier in *Chambers USA*, is described as a "wise counselor" and "one of the titans of the litigation Bar." *Chambers UK* describes co-head Dan Ornstein as having "an understanding of the law that allows him to get to the heart of an issue without over-complicating things."

Areas of Focus

- International Privacy Issues
- Drafting, Implementing, Reviewing and Amending Global Employment Policies
- Whistleblowing & Retaliation Claims
- Cross-Border Reductions in Force and Restructurings
- International Bonus Plans and Other Executive Compensation and Benefits Issues
- Multi-jurisdictional Employee Investigations
- Global Diversity Programs
- Expatriate Legal Issues
- Employee Aspects of Cross-Border Mergers and Acquisitions
- Offshoring and Global Resourcing

Proskauer Contacts:

For more information please contact the following at Proskauer.



Daniel Ornstein
Partner
London
44.20.7539.0604
dornstein@proskauer.com



Bettina B. Plevan
Partner
New York
212.969.3065
bplevan@proskauer.com



Yasmine Tarasewicz
Partner
Paris
33.1.53.05.60.18
ytarasewicz@proskauer.com



Erika Collins
Partner
New York
212.969.3555
ecollins@proskauer.com



Cécile Martin
Special International Labor &
Employment Counsel
Paris
33.1.53.05.69.26
cmartin@proskauer.com



Ying Li
Partner
Beijing
86.10.8572.1888
yli@proskauer.com



Ronald Meisburg
Partner
Washington, DC
202.416.5860
rmeisburg@proskauer.com



Peta-Anne Barrow
Special International Labor &
Employment Counsel
London
44.20.7539.0638
pbarrow@proskauer.com



Kristen J. Mathews
Partner
New York
212.969.3265
kmathews@proskauer.com



Katharine H. Parker
Partner
New York
212.969.3009
kparker@proskauer.com



Jeremy C. Leifer
Partner
Hong kong
852.3410.8048
jleifer@proskauer.com



Jeffrey D. Neuburger
Partner
New York
212.969.3075
jneuburger@proskauer.com



Lijuan Hou
Associate
Beijing
86.10.5737.2617
lhoul@proskauer.com



Jeremy M. Mittman
Associate
Los Angeles
310.284.5634
jmittman@proskauer.com

Beijing

Suite 5102, 51/F
Beijing Yintai Centre Tower C
2 Jianguomenwai Avenue
Chaoyang District
Beijing 100022, China
t: 86.10.8572.1800
f: 86.10.8572.1850

Boca Raton

2255 Glades Road
Suite 421 Atrium
Boca Raton, FL 33431-7360, USA
t: 561.241.7400
f: 561.241.7145

Boston

One International Place
Boston, MA 02110-2600, USA
t: 617.526.9600
f: 617.526.9899

Chicago

Three First National Plaza
70 West Madison, Suite 3800
Chicago, IL 60602-4342, USA
t: 312.962.3550
f: 312.962.3551

Hong Kong

Suites 1701-1705, 17/F
Two Exchange Square
8 Connaught Place
Central, Hong Kong
t: 852.3410.8000
f: 852.3410.8001

London

Ten Bishops Square
London E1 6EG, United Kingdom
t: 44.20.7539.0600
f: 44.20.7539.0601

Los Angeles

2049 Century Park East, 32nd Floor
Los Angeles, CA 90067-3206, USA
t: 310.557.2900
f: 310.557.2193

New Orleans

Poydras Center
650 Poydras Street
Suite 1800
New Orleans, LA 70130-6146, USA
t: 504.310.4088
f: 504.310.2022

New York

Eleven Times Square
New York, NY 10036-8299, USA
t: 212.969.3000
f: 212.969.2900

Newark

One Newark Center
Newark, NJ 07102-5211, USA
t: 973.274.3200
f: 973.274.3299

Paris

374 rue Saint-Honoré
75001 Paris, France
t: 33.(0)1.53.05.60.00
f: 33.(0)1.53.05.60.05

São Paulo

Rua Funchal, 418
26° andar
04551-060 São Paulo, SP, Brasil
t: 55.11.3045.1250
f: 55.11.3049.1259

Washington, DC

1001 Pennsylvania Avenue, NW
Suite 400 South
Washington, DC 20004-2533, USA
t: 202.416.6800
f: 202.416.6899