

2012 Survey

## Social Media in the Workplace Around the World 2.0



Proskauer 



## About Our Survey

---

Over the past two years, Proskauer and our global partners have collected nearly 250 responses from multinational businesses detailing their social media policies and practices. This report sets forth the results of our 2012 outreach, and compares it to the results of our groundbreaking 2011 survey, which has been cited by media outlets worldwide.

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 2.0

---

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

One year later, the use of social media has become increasingly accepted as a vehicle for conducting business. At the same time, hardly a week goes by without a story of a business facing issues related to its use of social media to vet potential employees and applicants or its attempts to monitor employees' social media use. Businesses also regularly risk reputational damage from an employee's viral tweet or Facebook post.

Indeed, despite the increasing use and maturity of social media, the ways in which workplaces deal with the use of social media is still in flux. Businesses are grappling with a medium that encourages informal and irreverent communications that are essentially permanent and have the potential to spread like wildfire. Likewise, the law is evolving to regulate developments on the virtual frontline. Around the world, social media usage raises difficult questions as to whether and how rules regarding workplace confidentiality, loyalty, privacy and monitoring apply to these forums, and, if so, how they are balanced against freedom of expression.

To help us understand business attitudes toward the use of social media and how the law continues to develop, following are the results of our second survey on emerging trends in practices on the use of social media in the workplace. Since last year, there have been notable developments in how businesses deal with social media usage, yet in some respects, the responses are the same as last year — this is also noteworthy.

To provide businesses with a global perspective on laws and regulations governing social media use in the workplace, in collaboration with select law firms around the world, we have included a brief summary of country-specific laws. This provides a valuable overview of the similarities and differences in various jurisdictions and how emerging legal developments are addressed globally. This year, we are delighted to add **China**, **India**, **Ireland** and **South Africa** to the list of jurisdictions covered.

## Summary of Findings and Developments

---

The notable changes that have emerged since last year are:

- Employers now have more positive attitudes towards social media, particularly for non-business use. This year, more than 40% of employers considered it an advantage to allow employees to use social media for both business and non-business use. Last year, the figure was just over 30%.
- There has been an increase in the number of employers that monitor usage of social media sites, from 27% to 36%.
- The number of employers that have dedicated social media policies has increased from 55% to 69%, with the figures suggesting that most of those who have introduced new policies have them covering usage both at work and outside of work.
- Like last year, just under half of all employers have had to deal with misuse of social media by employees (or former employees). To understand this issue and how businesses are dealing with it, this year we asked a number of additional questions. Our results revealed that:
  - Despite this high level of employee misuse, only about one-third of employers currently provide training on appropriate use of social media.
  - Just over one-quarter of abuse was by former rather than current employees.
  - Only 17% of employers have termination provisions with express protections against misuse of social media following employees' departure.

In some respects, the findings this year are similar to those from our 2011 survey, suggesting that after a few years of rapid development, some permanent traits are emerging in relation to the use of social media at work. In particular:

- More than three-quarters of respondents use social media for business—consistent with the figure from our last survey—albeit, 10% of this year's responders stated that they have only started doing so in the past year. This is a slower rate of adoption than in previous years which suggests that the adoption of social media for business purposes is reaching saturation point.
- The number of employers that allow all employees access to social media sites at work for non-business use remains at around one-half, and about one-quarter of businesses allow some, but not all, employees access to social media sites at work for non-business use.
- Just over one-quarter of employers block employee access to social media.
- About one-third of businesses have had to take disciplinary action against an employee for misuse of social media.

## Best Practices

---

Perhaps the most notable aspect of our survey is that despite local legal and cultural differences, there is a striking degree of commonality across the world as to the best practices for dealing with social media usage in the workplace. Here are our 5 key recommendations:

- Have a dedicated and well-communicated policy on social media use that clearly sets out acceptable and unacceptable usage, both inside and outside the workplace as well as after employment comes to an end. The policy should be implemented in accordance with and comply with local requirements, especially privacy laws. As well as the many advantages of having clear rules as to what employees can and cannot do, without such policies, it can be very difficult to lawfully sanction employees for misuse of social media.
- If employers choose to monitor social media usage by employees at work (and our survey shows that many employers do), have clear, express and well-communicated policies about the extent and nature of the monitoring. Ensure they comply with and are implemented in accordance with local requirements (again, especially privacy laws).
- Any monitoring should go no further than is necessary to protect the employer's business interests and should be conducted only by designated employees who have been adequately trained to understand the limits on what monitoring is permissible and comply with local privacy requirements, including in respect of the safe storage, confidentiality of and onward transfer of personal data.
- Exercise extreme caution before relying upon information on social media sites to make employment-related decisions, such as decisions about recruitment and discipline. In addition to the danger of such information being inaccurate, relying upon such information creates the risk of unlawful discrimination, breaching data privacy requirements and infringing individuals' rights to privacy. If businesses nonetheless wish to rely on such information, have clear processes and policies in place to mitigate such risks.
- Based on recent cases from around the world, an emerging issue is misuse of confidential information by employees via social media. As well as addressing this issue through social media policies, it would be best practice to amend provisions dealing with misuse of confidential information to explicitly cover misuse via social media.

## The Law Around the World

---

Notwithstanding local differences, there is a high degree of correlation among the approaches taken in different jurisdictions to workplace use of social media. In order to provide an overview of the current situation, which continues to develop rapidly, we have provided a synthesized summary of responses to some of the most frequently asked questions by focusing on commonality around the world as well as pointing out local differences where these exist. The jurisdictions covered are: **Argentina, Brazil, Canada, China, The Czech Republic, France, Germany, Hong Kong, India, Ireland, Italy, Japan, Mexico, Singapore, South Africa, 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 by this survey, the answer is yes, but with constraints on the extent to which monitoring is permissible, as well as guidelines to ensure the monitoring is lawful. As to monitoring social network 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.

While there are no laws or statutes addressing the specific issue of monitoring social media usage, in the U.S., the National Labor Relations Act plays a pivotal role. As a result, the common approach is to apply general legal principles, especially drawing analogies from case law pertaining to other technologies (such as email). In most jurisdictions, the courts 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 network surveillance.

## What Limits and Considerations Apply to Employers' Monitoring of Social Network 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, the best practice in most jurisdictions is that employers should take the following steps if they monitor employees' use of social media sites:

- Put in place clear, well-defined and well-communicated policies or contractual provisions concerning the appropriate use of social media sites and the sanctions for noncompliance.
- 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, and not disseminated further nor stored for any longer than is necessary.
- Train management and employees in the correct use of information technology.
- 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 sites 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, employees must explicitly agree to company policies that must clearly state the applicable rules in relation to monitoring social network usage.

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

**Canada:** Surveillance of employees' use of social media sites by the employer is allowed; 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 in the employment context, and specifically upon the monitoring of social media use, recent jurisprudence suggests an interest in limiting the types of cases in which it applies.

**China:** Employers should only monitor social media use by employees and deal with the data collected in ways that comply with the interest and moral standards of the society. In addition, a policy involving monitoring social network 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 of the monitoring 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 noncompliance, 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 (although 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. Guidelines state that employers should conduct due diligence to determine whether employee monitoring is the best option given the risks and activities the employer seeks to manage. The guidelines also recommend that employers should take into consideration the views expressed by employees when determining the parameters of any workplace monitoring, which would include the monitoring of social network 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 network 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.

**Ireland:** The local data privacy agency has issued guidelines 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 possession of data and the need to ensure that any encroachment on an employee's privacy is fair and proportionate. Staff must be informed of the surveillance.

**Italy:** Employers are generally not permitted to monitor the content of social media. However, an employer may prohibit the use of social media sites during work hours and monitor social media sites to determine whether an employee has used them in breach of any policies (and to 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 media 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 the use of social media at work must be part of a policy which clearly sets out the extent to which use of social media 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 network sites on company devices without prior notice or consent should be clearly stipulated in employment contracts or company regulations.

**Mexico:** As a rule, an employee's prior knowledge of and consent to a social network surveillance policy is sufficient for the lawful monitoring of social media usage in this jurisdiction.

**Singapore:** Surveillance of employees' use of social media sites by the employer is allowed; however, such monitoring must be reasonable and not rise to the level where it would be deemed harassment. The law may develop in the next year or so, since on 15 October 2012, a Personal Data Protection Bill was passed. The new law will go into effect January 2013, but there will be a transition period of a further 18 months before the new rules become enforceable.

**South Africa:** An employer can monitor social media usage if it has either obtained written consent from its employees, or (very broadly), where it does not have consent, in order to monitor or investigate unauthorized use of its telecommunications system. In order to avoid any disputes about whether employers are entitled to monitor their employees' social media activities on employer equipment, employers should include a clause in employment contracts (or in another document through which employees provide clear, written consent) stating that they are entitled to intercept and monitor all communication and activities on all electronic devices that they provide to their employees. In addition, it is best practice to enact workplace policies that clearly describe the conduct expected of employees when using social media sites.

**Spain:** Employers are permitted to monitor the time spent by employees on social media while they are at work (provided that they 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 media 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 Czech Republic:** Employers must inform employees of any monitoring scheme including the purpose and scope of the surveillance. The Czech Republic further requires that employers must have a serious reason to warrant the surveillance of social media usage.

**The Netherlands:** Where a company has a works council, the works council must be consulted with regard to any policy on social media that the company wishes to implement. In addition, the Dutch data protection authority should be notified about any monitoring.

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

**United States:** Broadly, any monitoring of social network 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. Therefore, policies and practices should clearly articulate the legitimate business interests 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 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 with respect to section 7 activities, may help defeat employee claims that the policy restricts 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 an employee's right to privacy in many jurisdictions); rather, the prohibition would stem from the employer's general right to require employees to devote all of their working hours to 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, supported by cogent business reasons such as promoting employee productivity (**The Netherlands** and **Mexico**) 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, with **Mexico** reporting that about one-third of companies have such bans in place. A few potential pitfalls are still worth noting, however, such as the rules in place in **Argentina** and **Japan**, which allow policies banning the 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 media 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 as to when and how information found on social media sites can be used by an employer for disciplinary purposes. Indeed (as set out in the following paragraphs), 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 media sites when making decisions about recruitment and selection of candidates, generally because referring to social media sites in such a context would be an infringement of an individual's right to privacy. Similarly, in **Canada**, considering an applicant's social media in the recruitment and selection process risks violating privacy laws. Canadian privacy regulatory authorities have issued guidelines to organizations on how much information can or should be collected via 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 addition, a Private Members' Bill has been proposed in Nova Scotia prohibiting employers from requiring access to an individual's social media website (although Private Members' Bills rarely become law).

In **Mexico**, the theory of the "right to (digital) oblivion" holds that personal information from the past that is not of public value should not be considered in a job application, and that could be applied to exclude most information found on social media sites. At present, however, no legal instrument ensures the application of this right, and as a result it is not uniformly respected or enforced.

In the U.S., 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, French recruitment agents 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 avoid looking at social media sites when recruiting.

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 media sites in relation to disciplinary action, recruitment and selection, the following should be kept in mind (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, the Netherlands Association for Human Resources Management and Development of Organizations has developed a code of conduct, which, although drafted specifically for its jurisdiction, 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 media 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 Network Sites by Their Employees Outside of Work?

In no jurisdiction does an employer have the right to prohibit the use of social media per se. However, employees are not entitled to use social media to do things 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 media to make clear that employees can be held responsible (and can be disciplined) for work-related misconduct that they engage in on a social media site, even on their own time. In the U.S., although such limitations are possible, any such policies have to tread carefully to ensure they do not have the effect of infringing the rights of employees under section 7 of the NLRA.

## Recent Cases on Social Media Use and Misuse – The Right to Sanction Employees for Making Derogatory Remarks About Their Employer via Social Media

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:** In a case involving Peugeot Citroën Argentina S.A., an employee was dismissed for cause because he used his business email account to exchange inappropriate comments with a supplier of his employer<sup>1</sup>. However, in this case, the employer had authorized the use of email for personal use. As a result, the judge ruled that the dismissal was null and void and compelled the employer to pay aggravated severance to the employee for wrongful termination of his employment contract. In this case, the employer made a statement about the use of work tools. However, the scope of the policy was unclear and therefore, by permitting the use of emails for personal use without stipulating that employees should not make inappropriate comments, the employee's rights to free speech in a personal capacity trumped the employer's right to protect its business. Although this case related to email and not social network use, it is generally thought that the decision would apply equally to comments made via social media, and therefore highlights the need to adopt clear and specific policies about the use of social media.

**France:** French case law remains divided on the issue of an employer's right to sanction employees for social network postings. In two recent decisions, French courts ruled that employees posting insulting comments about their employers on a social media Web site could be terminated for fault and also fined for the offense of public insult. One decision was rendered by a Criminal Court<sup>2</sup> and the other by a Labor Court of Appeals<sup>3</sup>. A third decision, however, issued a different ruling based on similar facts.

The first decision, that of the Criminal Court of Paris<sup>4</sup>, involved a trade union member who posted a message on the Facebook wall of the trade union recognized by his employer. In the posting, he insulted both his employer and his supervisor. In response, his employer not only decided to suspend the employee, but also to file a complaint against him for public insult, a criminal offense. The Criminal Court of Paris ruled that all the elements of the offense were met and fined the employee €500, as well as awarding a symbolic €1 of damages to the company and the employee's supervisor. In justifying its decision, the Criminal Court explained that the comments posted exceeded the limits of acceptable criticism, including when criticisms are expressed in a union context.

---

<sup>1</sup> G.M. vs. Peugeot Citroën Argentina SA re: dismissal", Chamber of Appeals Room V, Sala V, 16/02/2012 – Published in ERREPAR

<sup>2</sup> January 17, 2012 # 1034008388/

<sup>3</sup> November 15, 2011 # 10/02642

<sup>4</sup> November 15, 2011 # 11/01380

In the second decision, a company dismissed an employee for posting insulting comments about her company on the social media wall of a former employee of the same company. The Court of Appeal of Besançon ruled that the employer was entitled to use the comments posted by its employee as a basis for the dismissal. The Court reasoned that although Facebook's purpose was to be a social network, the employee had not checked prior to posting if her friend's wall was set so that it was displayed only to her friends rather than the public at large. In fact, the wall was set so that anyone could access the comments. As a consequence, the comments posted on the social media Web site could not be considered private, which in turn meant that the dismissal was lawful.

On the same day, however, the Court of Appeal of Rouen held that the dismissal of an employee who posted negative comments about his superiors was unlawful, holding that there was no evidence that the posts could be read by people other than the "friends" of the employee. In other words, the Court ruled that given the privacy settings of the employee's Facebook account, the content of her wall had to be considered private.

In light of these decisions, and particularly the decisions of the Courts of Appeal in Rouen and Besançon, it is clear that the extent to which any posting is private is directly linked to whether an employer is entitled to discipline an employee about that comment. The corollary is that employees should check the relevant privacy setting before posting a derogatory comment and be aware that the more accessible the comment, the greater the entitlement of their employer to impose sanctions as a result of what is posted.

**South Africa:** In the case of *Mahoro v. Indube Staffing Solutions*<sup>5</sup>, the plaintiff was dismissed after a complaint by a colleague who said that after collapsing at work, Mahoro posted a note on Facebook about it, making it difficult for the colleague to work with him. In this case, the employer failed to establish that the Facebook communication had an adverse effect on the business of the employer or had damaged the working environment, and the plaintiff's dismissal was declared unfair. It is therefore clear that an employer who relies on content posted on a social networking site to justify disciplinary action must demonstrate that the employee has committed misconduct by posting the content.

**Spain:** In a case involving EasyJet<sup>6</sup>, an employee was dismissed after making offensive statements and comments against the company in his profile on Facebook. The company, following its internal regulations on the use of social media by employees, dismissed the employee on the grounds that its code of conduct expressly permitted it to take disciplinary measures in the event of offensive or defamatory remarks being made against the company. The High Court of Justice accepted as evidence the statements posted on Facebook and held the dismissal as fair. This case is a good illustration of the benefits of having clear, dedicated policies about the use of social media.

---

<sup>5</sup> [2012] 4 BALR 395 (CCMA)

<sup>6</sup> High Court of Justice of Madrid, dated May 25, 2011



In a case involving nurses working at a hospital,<sup>7</sup> an employee was dismissed after creating a profile and a user account on a social network, supplanting the identity of one of the managers of his employer and inviting other employees to join his list of friends. The material contained in the network profile included offensive comments about the manager of the company which were considered to constitute insults against the employer, all of which resulted in the dismissal of the employee for breach of the contractual duty of good faith and abuse of confidence. The High Court of Justice accepted as evidence the statements made on the social network, and the Court ruled the dismissal as fair.

**United Kingdom:** In November 2011, the Employment Tribunal in England grappled with the issue of the balance between privacy and freedom of expression and the protection of business interests in the context of social media in the case of *Crisp v. Apple Retail UK Limited*.<sup>8</sup>

Mr. Crisp worked in the Apple store. He made a number of Facebook posts referring to his work in expletive terms, complaining about technical problems with his iPhone and referring to an Apple “app” not working properly (again in expletive terms). Following a disciplinary hearing, Mr. Crisp was dismissed for gross misconduct on the grounds of bringing Apple into disrepute and making derogatory comments about Apple products and his work on Facebook. Mr. Crisp brought a claim against Apple that his dismissal was unlawful because his posts were private. The privacy setting on his profile meant that only his “friends” could see them. Therefore, he alleged that his dismissal was in breach of his right to privacy under the Human Rights Act 1998 (which, put broadly, incorporates the European Convention of Human Rights (the “Convention”) into English law). The Employment Tribunal accepted that section 6 of the Human Rights Act meant that, as a public authority, it must not act in a way which is incompatible with a right under the Convention.

In this case Mr. Crisp invoked two Convention rights: the right to privacy (under Article 8 of the Convention) and the right to freedom of expression (under Article 10). Both these Convention rights are qualified such that they can be interfered with where doing so is justified and proportionate.

As to the right of privacy, the Employment Tribunal determined that even though Mr. Crisp had limited access to his posts to his Facebook friends (in contrast to the decision of the Court of Appeal of Rouen) he could not have any reasonable expectation of privacy over them and that his right to privacy was therefore not engaged. This was because of the ease with which online comments by one person can be forwarded to others and the lack of control that a person who posts a comment has over how it is forwarded. The Employment Tribunal also held that even if Mr. Crisp’s right to privacy was engaged, there was no infringement of this right because the interference by Apple (in the form of dismissing Mr. Crisp) was justified and proportionate, especially with regard to Apple’s own legitimate interest in protecting its reputation.

---

<sup>7</sup> Decision of the first level judge in Murcia dated July 6, 2011

<sup>8</sup> (2011) ET/1500258/11

As to freedom of expression, the Employment Tribunal accepted the right was engaged but held that Apple's restriction of the right was justified and proportionate in the context of its need to protect its reputation. It was noteworthy that in reaching this conclusion the Employment Tribunal remarked that Mr. Crisp's comments were not the type that are particularly important to freedom of expression (such as, for example, political opinions), and they were clearly potentially damaging to Apple's reputation.

The Apple decision is consistent with another recent Employment Tribunal decision in the case of *Preece v. JD Wetherspoon*<sup>9</sup>, where Mr. Preece's dismissal, as a result of derogatory comments made on Facebook about customers, was held to be lawful. As in the *Crisp* case, the Employment Tribunal held that: Mr. Preece's comments were not in private, even though he had set his privacy settings so that only his Facebook friends could see them; and, even though his right to freedom of expression was invoked, his employer's restriction of the right was justified and proportionate in the context of its need to protect its reputation.

**United States:** In light of the way in which the NLRA applies to social media use in the workplace, the National Labor Relations Board (the "NLRB") has issued a number of decisions that impact the rights of employers to sanction employees for materials posted on social media.

Illustrative of these decisions is a complaint authorized by the NLRB's Acting General Counsel in the case of *Karl Knauz Motors, Inc., v. Robert Becker*<sup>10</sup>, involving a BMW car salesman who was fired for Facebook comments and pictures. These posts related to pictures and commentary critical of a sales event (where Mr. Becker objected to the fact that the employer made available only hot dogs and chips to customers). The pictures and commentary detailed in mocking terms a Land Rover accident at the employer's sister dealership located next door to the BMW dealership. After his dismissal, the salesman filed charges and the NLRB issued a complaint that he had been dismissed for carrying out a protected activity under section 7 of the NLRA. In particular, Mr. Becker asserted that he was dismissed in connection with his comments about the sales event (and not the Land Rover crash) and such comments were protected activities under section 7 of the NLRA, thus rendering his dismissal unlawful.

In his decision, the Administrative Law Judge analyzed the sales event and the Land Rover crash separately under the Act. As to the sales event, the Judge found that it was protected, concerted activity because evidence at the hearing established that the salespeople at the dealership had a meeting with management to discuss how the sales event was handled, and these concerns were discussed afterwards by salespeople. Even though the employee who was fired was the only one of the salespeople to post comments about the event on Facebook, this conduct was deemed protected because the complaint about the sales event highlighted things that could have resulted in reduced compensation

---

<sup>9</sup> (2011) ET/2104806/10

<sup>10</sup> [2011] Case No. 13-CA-46452

for the salespeople generally. The Judge, however, seemed to conclude that it was only barely protected, stating in his decision: “While it was not as obvious a situation as if he had objected to the [Employer] reducing their wages and benefits, there may have been some customers who were turned off by the food offerings at the event and either did not purchase a car because of it or gave the salesperson a lowering (sic) rating in the Customer Satisfaction Rating because of it; not likely, but possible.”

The Judge noted that the discharged employee had 95 friends, 16 of whom were employed by the employer. The employee acknowledged that his privacy settings allowed access to “friends of friends,” so the potential number of people who saw his posts about his employer could be well over 1,000 people or more.

The Judge went on to conclude that the salesman’s dismissal was not unlawful because the real reason the employer fired him was for posting material which made fun of the Land Rover accident.

The case is noteworthy because it illustrates the relative ease with which posts on social media can potentially fall within the scope of protected concerted activities under section 7 of the NLRA.

More generally, and in response to the increasing volume of decisions, in August 2011, NLRB Acting General Counsel, Lafe Solomon, issued a report explaining the rationale underlying the NLRB’s decisions in a sampling of the key social media cases<sup>11</sup>. On the basis of that report and the cases referred to in it, the current position in the U.S. holds that disparaging comments on social media about an employer, including supervisors, are generally protected, but they may lose the protection when they:

- Are unrelated to a dispute over working conditions;
- Focus only on the employer’s products or business policies, particularly if the criticism comes at a “critical time” for the employer;
- Are reckless or maliciously untrue;
- Are appeals to racial, ethnic or similar prejudices; or
- Are insulting or obscene public personal attacks that cross an undefined “I know it when I see it” line of propriety.

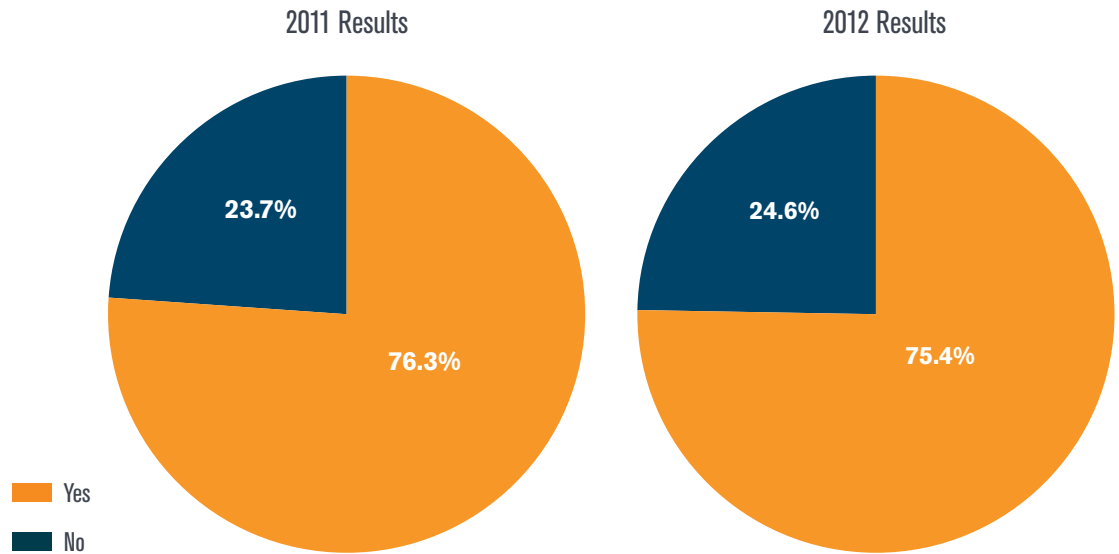
---

<sup>11</sup> OM 11-74 Report of the Acting General Counsel Concerning Social Media Cases

# The Survey Results in Full

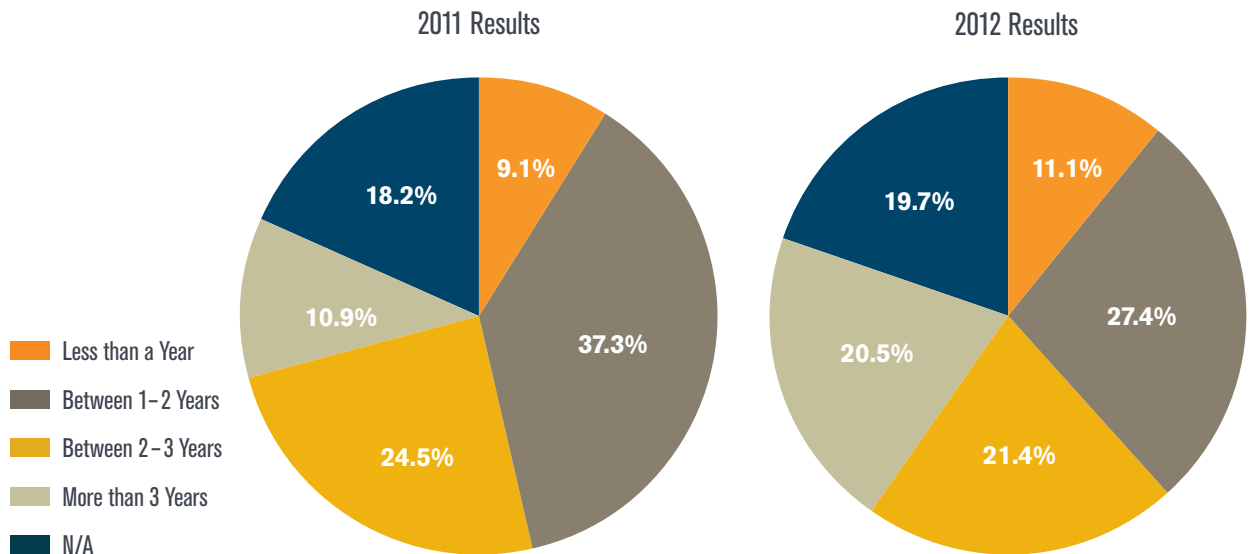
## Question 1:

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



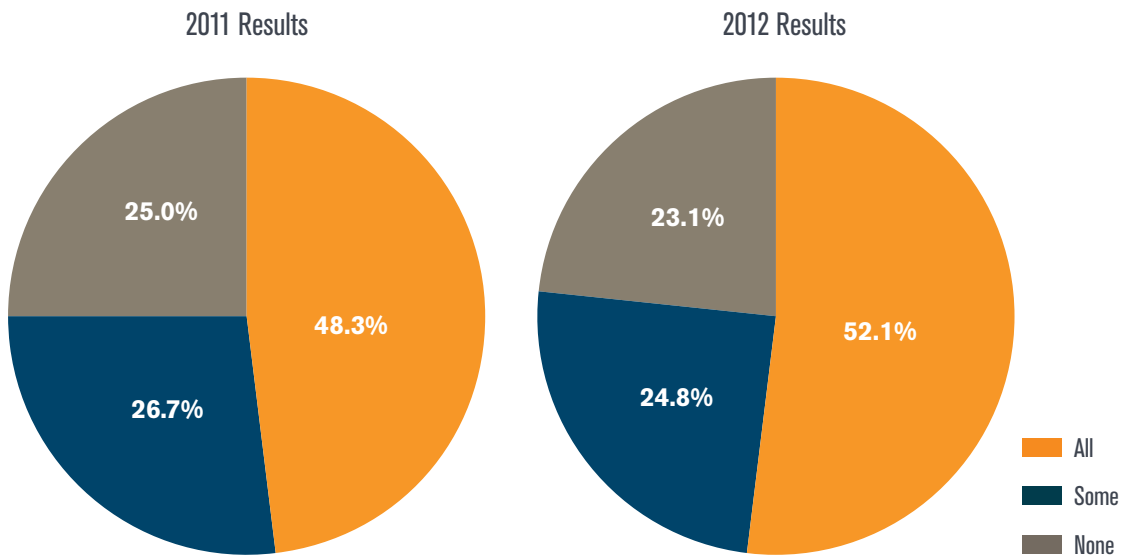
## Question 2:

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



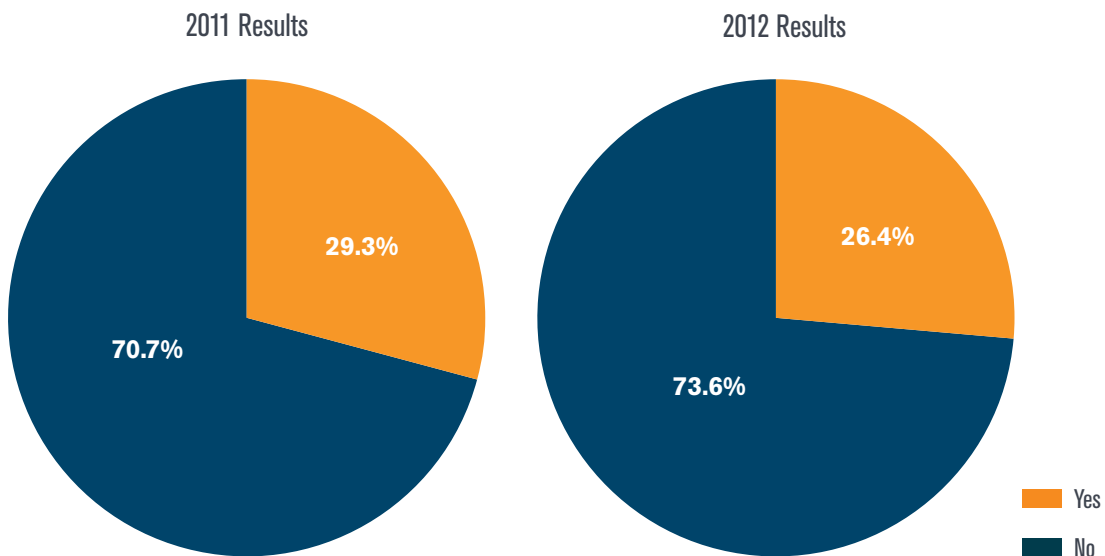
### Question 3:

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



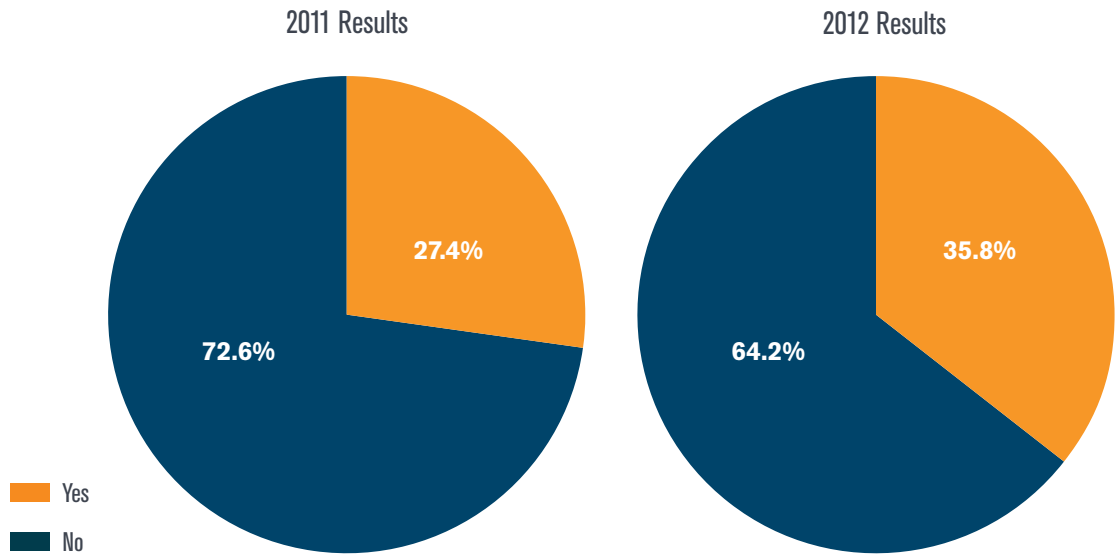
### Question 4:

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



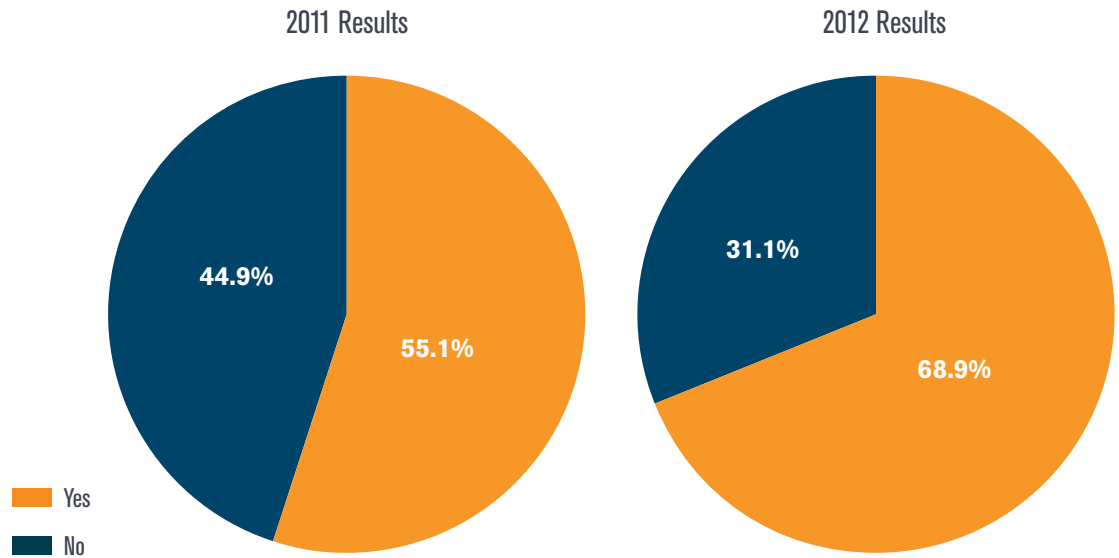
### Question 5:

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



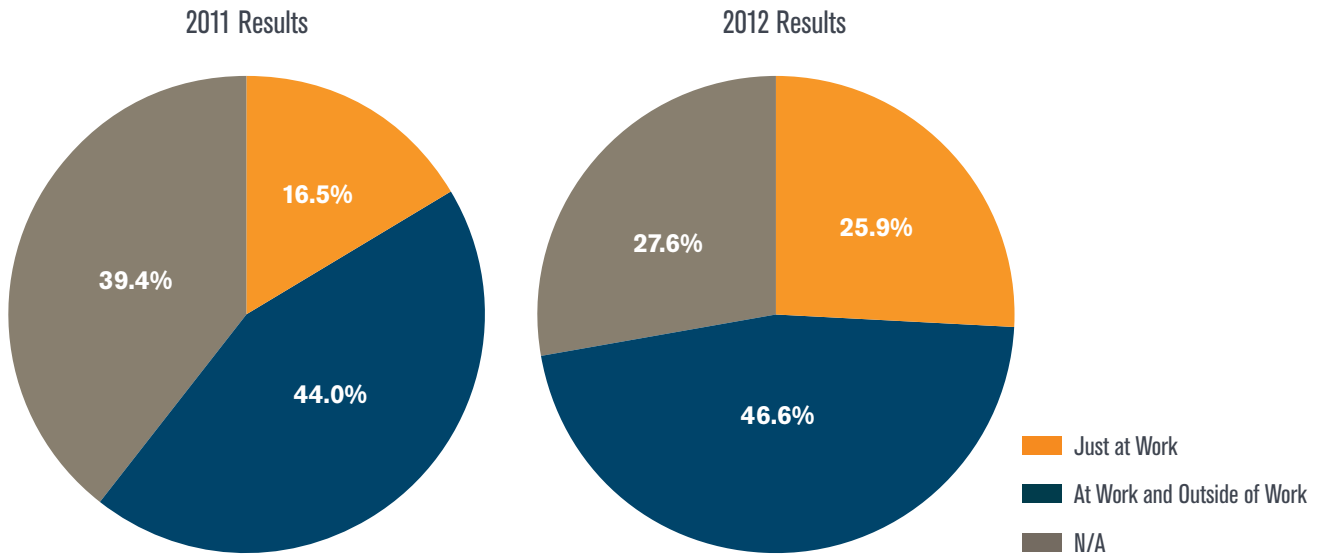
### Question 6:

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



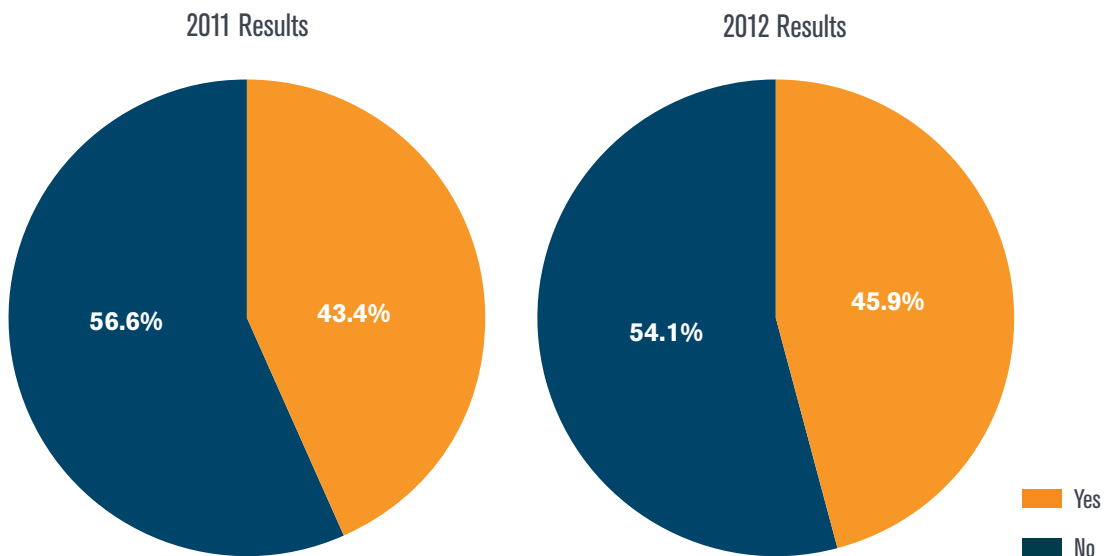
### Question 7:

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



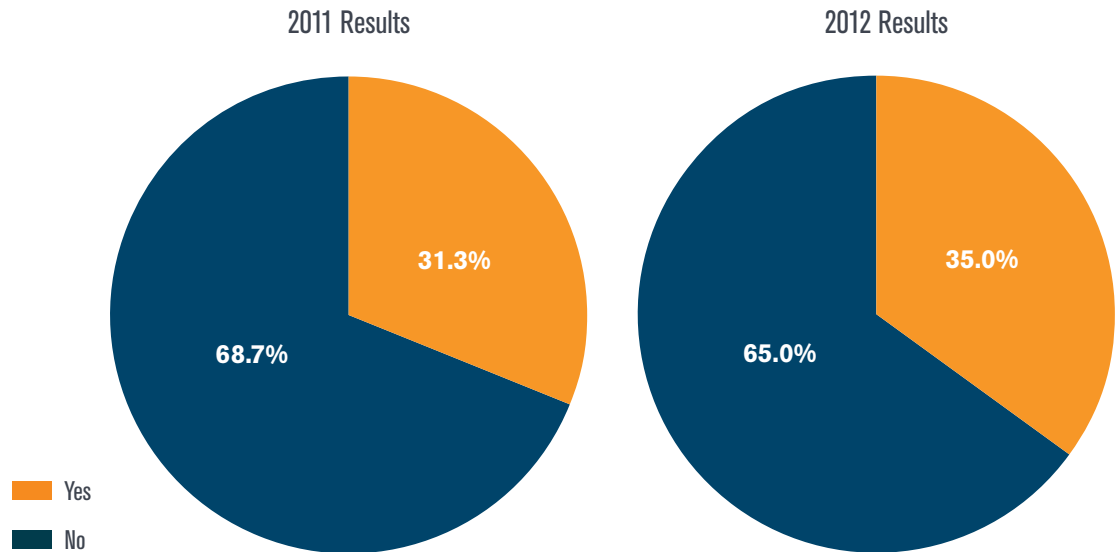
### Question 8:

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



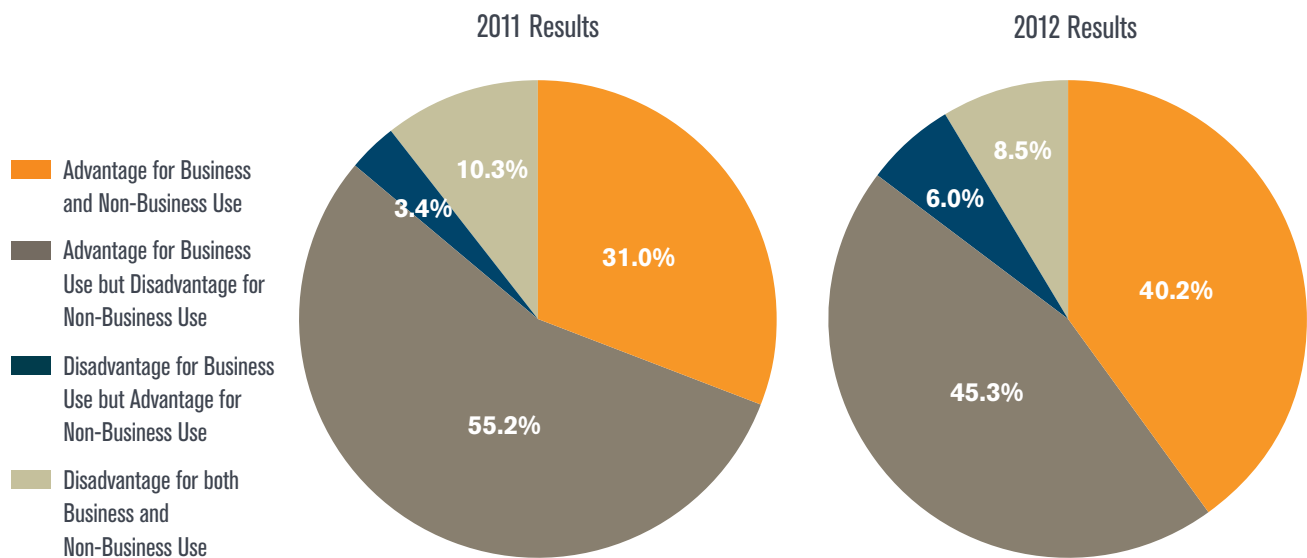
### Question 9:

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



### Question 10:

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?

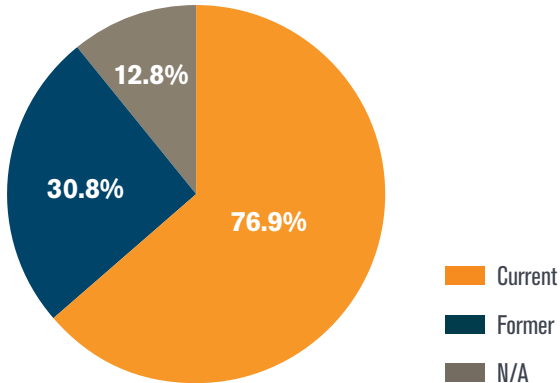




## Additional Questions for 2012

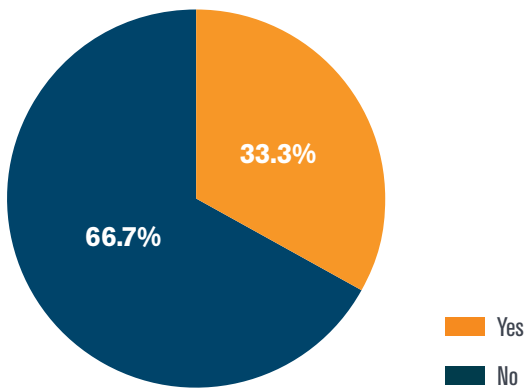
### Question 11:

Referring to Question 8, was the misuse of social media an issue caused by current employees or former employees?



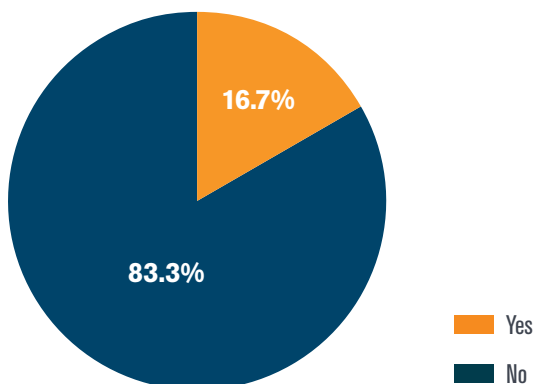
### Question 12:

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



### Question 13:

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



## 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:** Bridget McIlveen and Adam Kardash, Heenan Blaikie LLP (www.heenanblaikie.com)

**China:** Ying Li, Proskauer Rose LLP (www.proskauer.com)

**The Czech Republic:** Martin Kubánek and Veronika Odrobinova, Schoenherr (www.schoenherr.eu)

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

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

**Germany:** Burkard Göpfert and Thomas Winzer, Gleiss Lutz (www.gleisslutz.com)

**Hong Kong:** Ying Li and Jeremy Leifer (www.proskauer.com)

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

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

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

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

**Mexico:** Carlos Leal-Isla Garza, Leal-Isla & Horváth, S.C. (www.lealislacom.mx)

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

**Singapore:** Kelvin Tan and Jason Chen, Drew & Napier LLC (www.drewnapier.com)

**South Africa:** Ross Alcock, ENS (www.ens.co.za)

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

**United States:** Betsy Plevan, Ronald Meisburg and Katharine Parker (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



**Ying Li**  
Partner  
Beijing  
86.10.8572.1888  
yli@proskauer.com



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



**Peta-Anne Barrow**  
Associate  
London  
44.20.7539.0638  
pbarrow@proskauer.com



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



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



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



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



**Jeremy C. Leifer**  
Partner  
Hong kong  
852.3410.8048  
jleifer@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**

Ninth Floor  
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