Legal Matters®

Business Law
spring 2013

'Bring your own device to work' policies carry legal risks

More and more businesses are allowing employees to use their own laptops, tablets and smartphones for work, instead of providing the equipment themselves.

About a third of all large companies in the U.S. now have a "bring your own device" policy, and about half of smaller companies do.

These policies have a lot of advantages, but they can also create security and legal risks. If you have such a policy, or you're thinking of adopting one, it's wise to have a written agreement with your employees that will protect you if something goes wrong.

In fact, it's *always* wise for a business to have written agreements and policies about the use of personal technology, since employees today are increasingly likely to use their own devices for work purposes, whether it's officially allowed or not.

The basic advantage of a "bring your own device" policy is obvious – the company can save the cost of providing workers with expensive computer equipment.

But there are other advantages, too. Employees are usually more comfortable working with their own device, and there's no "learning curve" as workers gradually get used to the ins

continued on page 2

©istockphoto.com

Jones & Smith
123 Main Street
Boston, MA 00000
(617) 123-4567
www.website.com

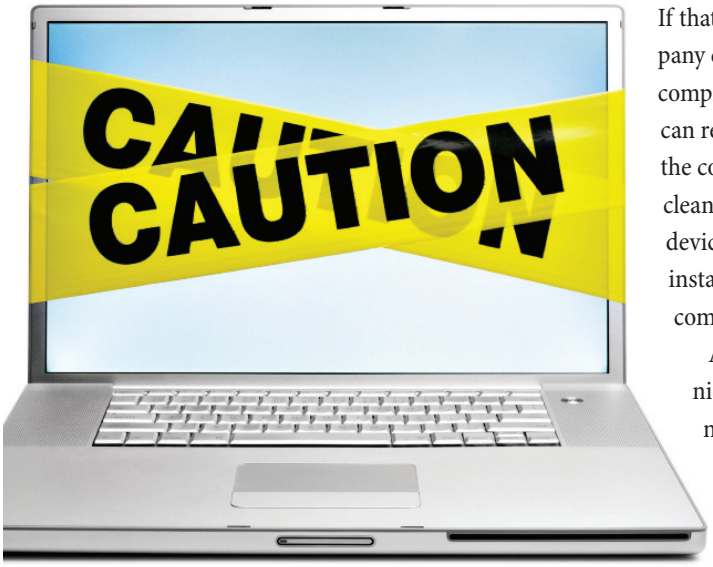
‘Bring your own device to work’ policies carry legal risks

continued from page 1

and outs of a different machine.

But the risks are very serious. Here’s a look at some of them, and the ways that employers need to protect themselves:

Security. Workers’ personal devices are much more likely to be lost or stolen. If that happens, sensitive company data and e-mails may be compromised. A written policy can require workers to allow the company to remotely wipe clean data from a lost or stolen device, and require them to install software enabling the company to do so.



©istockphoto.com

At the very least, companies can require workers to maintain password locks on phones.

Another issue is that there are many new laws requiring businesses to notify customers if there is a security breach, and companies should be aware of whether a lost or stolen personal device will trigger these laws.

Viruses. Statistically, personal devices are twice as likely as company-owned devices to become infected with malicious software. And viruses can spread throughout a company when the victim logs into a company network. A written policy can require workers to update their machines with the latest anti-virus software.

Who owns the data? If an employee leaves the company, who owns the data on the employee’s personal device? A written policy should make extremely clear that the company owns the data, and should also allow the company to retrieve the data if the employee leaves, and remove it from the employee’s machine. Otherwise, the company might be deprived of essential information and records.

This is tricky, because it’s not always easy for a company to extract work-related information from a personal device without extracting personal information as well. Unless the company is careful, it could wind up facing complaints of invasion of privacy from a former employee.

Sensitive information. There are many new laws that impose detailed restrictions on how a company stores sensitive data, such as credit card numbers, Social Security numbers, and driver’s license and bank account information. You’ll need to determine whether you can legally allow employees to store this type of data on their personal devices. If not, you’ll want a written agreement to prohibit employees from doing so, so you can show that you made every effort to protect the information.

Other laws require certain types of information to be encrypted or securely destroyed, such as health records and consumer credit reports. And if you enter into a non-disclosure agreement with another company, you’ll need to consider whether the agreement allows storage of information on personal devices.

Trade secrets. What happens if an employee goes to work for a competitor and shares confidential information that was on his or her device? In the past, it was easy to show that an employee did something wrong if he or she copied company data onto a personal computer, but if a company explicitly allows or even encourages employees to do so, it may make it harder to prove in court that the information was protected. This needs to be covered in a written agreement.

The reverse is also true; companies need to protect themselves from being sued for misappropriation of trade secrets if a new employee shows up for work with confidential information from a former employer on a personal device.

Overtime problems. Companies need to be aware that if employees are responding to e-mails and otherwise performing work at home after-hours on a personal device, this can lead to claims for overtime pay. One way to solve this is for a written agreement to say that e-mails should be responded to only during working hours, unless a supervisor has given specific instructions otherwise.

In general, a written policy should emphasize that using a personal device for work is a privilege, not a right – and the privilege is contingent on the employee observing the sorts of basic requirements outlined above that are necessary to protect the company’s interests.

It’s wise to have a written policy about the use of personal technology, since employees today are increasingly likely to use their own devices whether it’s officially allowed or not.

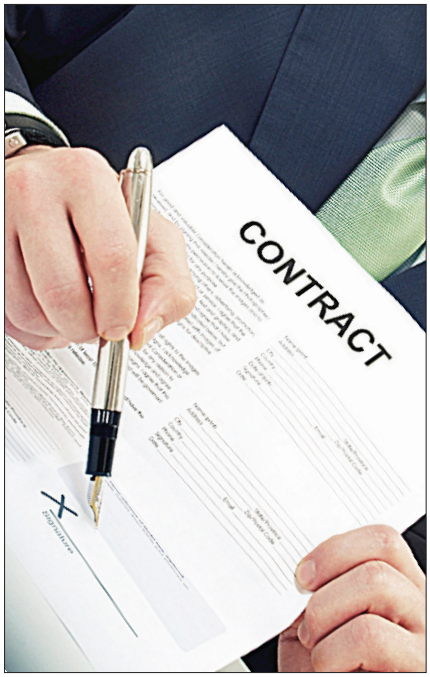
What arbitration clauses should say (and usually don't)

A large number of business contracts contain some "boilerplate" language to the effect that any disputes will be resolved by arbitration. That's fine – but a good arbitration clause should be a little more specific, and should resolve the most common sorts of questions that tend to arise when problems actually *do* go to arbitration.

After all, the point of an arbitration clause is to provide a quick, inexpensive resolution of disputes. So why allow an actual arbitration to be bogged down by unnecessary and preventable delays and issues?

A good arbitration clause should say:

- How will the arbitrator be selected? Will each side choose from a list provided by a specified organization? What happens if they can't agree?
- Must the arbitrator have a specific expertise or other qualifications?
- Will the proceedings be covered by a confidentiality requirement?
- Must the two sides go to mediation first, to try to resolve the dispute before arbitration? If so, how will a mediator be selected?
- Where will the arbitration be held? If the parties are far apart geographically, can some or all of the proceedings be held electronically?
- Will court rules of evidence apply? Or can the arbitrator decide on the rules?
- Is there a time limit during which the arbitration must occur?
- What powers does the arbitrator have? Can he or she just award money? What about punitive damages? What about equitable relief, i.e., ordering one party to do something or not do something?
- Will the arbitrator have the power to order equitable relief for one side on an emergency basis, before the case as a whole is decided?
- If one side claims that a particular dispute isn't covered by the arbitration clause, can the arbitrator decide whether it's covered?
- Who will pay the arbitrator's fees?



©istockphoto.com

You can still use a "boilerplate" clause in most cases, but a slightly longer version that answers these questions will go a long way toward guaranteeing the sort of quick and easy resolution of disputes that prompted you to want arbitration in the first place.

Important news if you're applying to get a patent

As of March 2013, the way that patents are granted in the U.S. has undergone a radical change.

For more than 200 years, when two or more people claimed to have invented something, the key question was who actually invented it first. Starting now, however, the key question will be who was the first to file a patent application. This means that the second person to invent something might nevertheless "win" the patent simply by winning the race to the U.S. Patent Office.

This change is part of a new law called the America Invents Act.

This law also makes very big changes in the process by which someone can legally challenge the validity of someone else's patent.

If you're interested in obtaining a patent, there is now much more of a premium than before in acting quickly, before someone else gets the same idea.

New federal form needed for background checks

If you use an outside agency to perform background checks on employees or job applicants, then a federal law called the Fair Credit Reporting Act requires you to provide a form to any person if you take adverse action against them based on the results of the report. This form summarizes the rights of the employee or applicant under the law.

You should note that a new form is required to be used starting in 2013. If you're still using the old form, you should discard it and begin using the new form.

The main reason for the change is that the old form was issued by the Federal Trade Commission. As of January 1, 2013, regulation of this aspect of the law has been moved to the federal government's new Consumer Financial Protection Bureau.

The Bureau issued its own form; among other things, the new form provides contact information for the Bureau as well as the FTC.

We welcome your referrals.

We value all our clients. And while we're a busy firm, we welcome all referrals. If you refer someone to us, we promise to answer their questions and provide them with first-rate, attentive service. And if you've already referred someone to our firm, thank you!

Should your company adopt a Roth 401(k) plan?

The new tax law that resolved the "fiscal cliff" back in January will prompt many more companies to offer their employees a Roth 401(k) plan in addition to a traditional 401(k) plan.

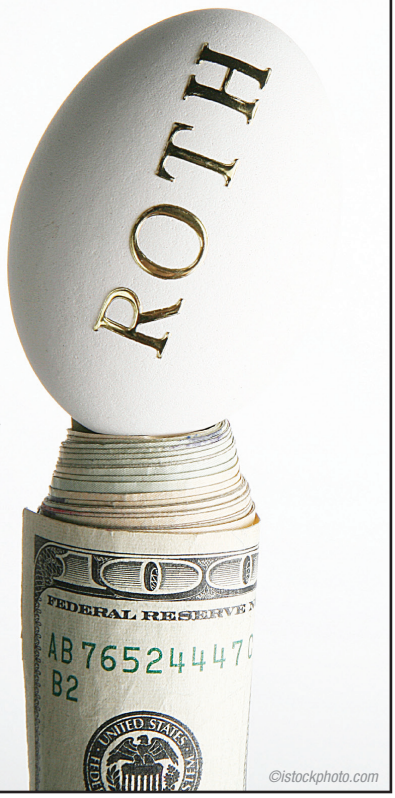
In a traditional 401(k) plan, employees contribute pre-tax earnings, the assets grow tax-free, and an employee can withdraw them at retirement age and pay ordinary income tax on the withdrawals.

With a Roth 401(k), employees contribute *post*-tax earnings, but when they withdraw the assets years later, the withdrawals are tax-free.

Roth 401(k)s have been around for a few years, but they haven't been very popular, in part due to numerous restrictions on the ability of employees to transfer existing 401(k) assets into a Roth account. But the new fiscal cliff law allows employees to freely convert any or all of a traditional 401(k) into a Roth 401(k), simply by paying income tax now on the amount transferred.

As a result, Roth 401(k)s may soon become a very desirable employee benefit. They will appeal to anyone who expects to be in a higher tax bracket at retirement, or who expects tax rates to increase generally. For complex tax reasons, they may also appeal to employees who plan to leave the account to their heirs as part of their estate planning.

Roth 401(k)s will often be more attractive than Roth IRAs, because (1) the annual contribution limits are much higher for a Roth 401(k) than for a Roth IRA, and (2) high-income individuals can't make Roth IRA contributions, but they can make Roth 401(k) contributions.



Jones & Smith
123 Main Street
Boston, MA 00000
(617) 123-4567
www.website.com