Legal Matters®

Business Law
spring 2015

You may need a policy covering employees' use of cloud storage

Employees are discovering that cloud storage services are a great way to access work-related data at home and on the road, and to collaborate with co-workers, especially those who work remotely.

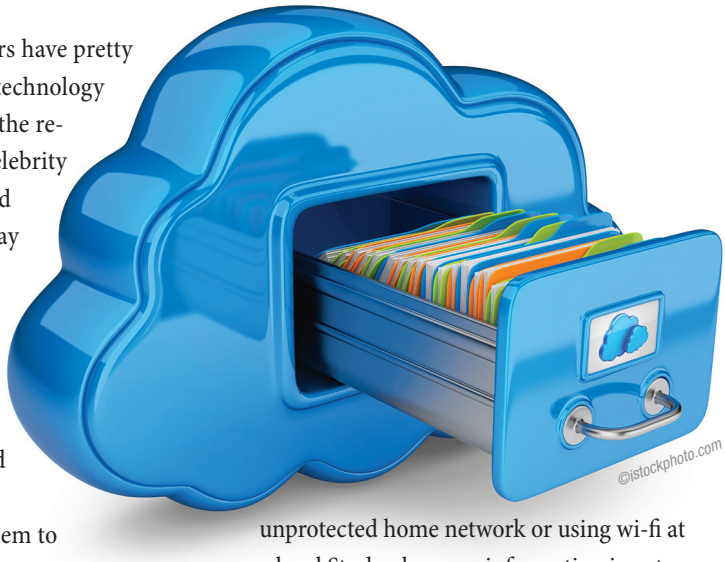
Unfortunately, they're also a great way to make your confidential data insecure – which is why you may need a thoughtful policy covering their use.

Cloud services allow a user to log into an account, upload documents or files, and then access or download them from any device, anywhere and at any time. Users can sync folders across devices, and can also share or sync files with others.

Common examples include Dropbox, Google Drive, SkyDrive and Cubby.

While these services can greatly enhance productivity, they also pose risks, because once employees upload data to the cloud, it's no longer on your system.

Most cloud providers have pretty good security, but no technology is foolproof – witness the recent release of nude celebrity photos that were stored in the cloud. And it may not even be necessary for hackers to "crack" a sophisticated system. One common hacker technique is to steal usernames and passwords from less-secure sites and use them to try to log into more secure sites. Since many people use the same passwords for multiple sites, this sometimes works.



Also, the whole idea of cloud storage is to be able to access data remotely, and your security is only as good as the network your employees are using at that moment. If an employee is accessing sensitive data on an unprotected home network or using wi-fi at a local Starbucks, your information is not secure.

A hack of company data can be devastating. In the recent Sony case, stolen data included employees' salaries, Social Security numbers, private medical information and much more. Sony is now being sued by employees in a class action.

continued on page 2

ALLRED, BACON, HALFHILL & YOUNG, PC

11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com

©istockphoto.com

Be careful – a 'letter of intent' may sometimes be binding

Businesspeople who have agreed on the general terms of a deal often sign a "letter of intent" that lays out these terms in writing. The idea is to make sure that everyone is on the same page while a formal contract is being drafted.

But what happens if you sign a letter of intent with someone, and then they walk away from the deal? Is that okay?

In general, the answer is yes – a letter of intent isn't a binding contract; it's merely an expression of a plan to negotiate a binding contract.

But that's not always true. Sometimes a letter of intent is so specific and leaves so little out that it can legally be considered a contract in itself.

For instance, in one case involving a sale of real estate, the buyer and seller signed a letter of intent that included a description of the property, the sale price, the deposit and title requirements, and the time and place of closing. It said that the buyer's offer was accepted, and that the buyer and seller "shall" sign a sale contract that was satisfactory to both sides.

Before signing the sale contract, though, the seller changed her mind and agreed to sell the property to someone else.

The buyer sued, and the Massachusetts Supreme Court sided with him. It said that while the letter of intent wasn't a formal contract, it was so specific and clear that it amounted to a binding agreement by the seller.

If you're signing a letter of intent, you might want to think carefully about the language, if it's very important to you to (1) preserve your right to back out or (2) make it as difficult as possible for the other side to back out.

Some letters of intent solve this problem with a "withdrawal fee." That is, they say that the letter isn't a binding contract, but if one side doesn't sign a binding contract on the stated terms by a certain date, he or she must pay a certain amount of money as a penalty.

You may need a policy covering cloud storage

continued from page 1

Another risk is that cloud services make it easy for an employee who is planning to go to work for a competitor to steal confidential information. In the past, businesses were often able to catch such employees, because they would typically e-mail lots of files to a personal e-mail account in the days before they left. But if an employee has routinely synced his or her computer with a home device, it's much harder to prove they did something wrong.

Employees can even set up a script at home so that every time a file is added to Dropbox, it is printed on their home computer.

If you ever bring a lawsuit against a competitor for theft of trade secrets, one of the things you will have to prove is that the information was actually "secret," and that you took reasonable steps to keep it confidential. If you don't have a policy that limits employees' ability to upload and share data in the cloud, that's much harder to prove.

One way to protect yourself is to limit your company to one cloud provider. It's much easier to maintain security with one company than it is if you let employees do their own thing with whatever providers they choose – especially if the cloud service you work with can give you reports on employee usage.

It may also be a good idea to have a written cloud storage policy and have employees sign off on it.

Among other things, such a policy could say that employees may not upload or share data using the cloud without approval by management, may not use a cloud service that's not approved by management, may access cloud data only when they have a secure connection, may not download data to home devices or share data with anyone outside the company, and may not share their login credentials with anyone (including co-workers).

Does your insurance cover a data breach?

Given the rapid increase in data breaches – affecting not only Fortune 500 companies but smaller businesses as well – it's worth checking whether your current insurance policy covers cyber losses.

That's especially true now that almost every state requires companies to notify customers if their data has been compromised.

A growing number of insurers are now offering cyber-liability policies. These typically cover the costs of investigating a data breach and notifying customers, loss of business and reputation, and future credit monitoring.

A recent study by the Ponemon Institute found that businesses with fewer than 10,000 customer records are more likely to be hacked than businesses with over 100,000 records, in part because they're less likely to have robust defenses against hackers.

The study also said that in data breaches involving more than 500 customers, the average cost to a company was $5.9 million.

‘Puffery’ on product label was okay, court says

A manufacturer isn’t allowed to make false or misleading statements in its advertising or on a product label. But in a recent case involving the Gerber baby food company, a California court ruled that claims made on its labels, while vague and open to interpretation, were not over the line.

Gerber said on some of its labels that its products were “an excellent source” of various vitamins and minerals, that they provided “natural immune support” and helped create “healthy growth and development,” and that they contained “no added sugar.”

A California consumer brought a class action, claiming that the statements about vitamins and health were misleading. She argued that while the statements may have been literally true, consumers were tricked into paying a premium price for Gerber products even though other baby food products contained essentially the same health benefits.

She also argued that while the claim about “no added sugar” might be true, it was misleading because consumers would naturally assume that the baby food was low in calories – which it wasn’t.

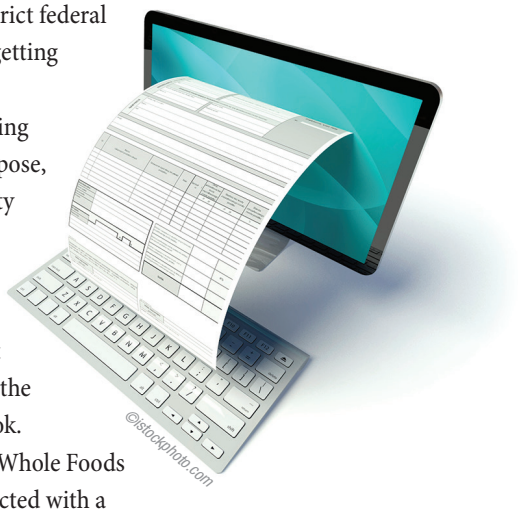
But the court threw out the lawsuit. It said that Gerber’s statements were factually accurate, and the fact that one consumer might be misled about what they implied didn’t make them illegal.

A consumer can’t bring a lawsuit unless she can prove that a broad swath of the public was actually duped into buying a product they otherwise wouldn’t have, the court said.

Beware of off-the-shelf forms for conducting background checks

A company can conduct background checks on job applicants, but there are strict federal laws governing how to go about getting applicants’ permission to do so.

Increasingly, businesses are using “off-the-shelf” forms for this purpose, or are contracting with third-party vendors to set up an online job application process.



The problem is that if the forms or the online services don’t comply with the letter of the law, the company itself may be on the hook.

This happened recently to the Whole Foods supermarket chain, which contracted with a vendor to set up an online application system.

The vendor required applicants to fill out a background check disclosure and consent form, as required by the law, but it allegedly violated the law by putting release-of-liability language on the same form, rather than on a separate form.

Companies that violate the law can be required to pay damages of up to $1,000 per applicant, plus other damages in some cases.

Other businesses that have been hit with similar lawsuits recently include Home Depot, Disney, Domino’s Pizza, CVS, K-Mart, Uber, Dollar General and Publix Super Markets.

Companies can’t prohibit workers from discussing salaries

A company can’t prohibit its workers from disclosing and discussing their salaries, according to a federal appeals court in New Orleans.

That’s because federal labor law says that employees always have a right to talk about the terms and conditions of their employment. And that’s true regardless of whether the employees belong to a union.

The case involved a non-union trucking company in Fort Worth, Texas that made its workers sign a confidentiality agreement. The agreement said that workers could not reveal any “financial information” or “personnel information” to anyone outside the company.

©istockphoto.com

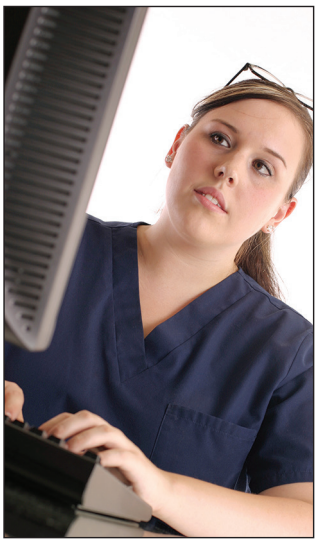
Although the agreement never specifically mentioned salaries, the court said it was nevertheless illegal because workers could reasonably assume that salary information was included.

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!

This newsletter is designed to keep you up-to-date with changes in the law. For help with these or any other legal issues, please call our firm today. The information in this newsletter is intended solely for your information. It does not constitute legal advice, and it should not be relied on without a discussion of your specific situation with an attorney.

ALLRED, BACON,
HALFHILL & YOUNG, PC
11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com


©istockphoto.com

Businesses sued for disclosures of health care information

The federal law called HIPAA requires anyone who has access to medical information to keep it confidential. Businesses that violate the law can face penalties from the government. A big new threat, though, is that recently some courts have also started allowing people whose information was improperly disclosed to sue for damages in court.

This is significant, because the HIPAA law applies not only to doctors and hospitals but also to businesses that have even occasional access to medical data. This includes dentists, pharmacies, chiropractors, rehab facilities, insurers, data processing companies, transcriptionists, accountants and consultants who work with medical clients, and others.

In one recent case, a Walgreens pharmacist improperly accessed a patient's records and allegedly disclosed them to her husband. The patient was the husband's ex-girlfriend, with whom he had a child. The pharmacist apparently found information about whether the patient had a sexually transmitted disease and whether she stopped taking birth control pills shortly before becoming pregnant.

The Indiana Court of Appeals approved a jury award of more than $1 million against Walgreens for the incident.

In another case, a woman specifically asked her gynecologist not to provide her medical information to a man she was involved with. But when the man's lawyers served the gynecology practice with a subpoena during a paternity lawsuit, the practice handed over the records – without telling the woman or informing the judge in the case.

The Connecticut Supreme Court said that the woman could sue the medical practice for money damages for the breach of confidentiality.

If anyone in your business has access to medical information, it's a good idea to review your protocols for keeping it private.