EPSTEIN BECKER GREEN

Take 5 VIEWS YOU CAN USE

LABOR AND EMPLOYMENT

This issue of *Take 5*, "5 Employment Law Considerations in 'The Cloud,'" was written by **Ian Carleton Schaefer**, Member of the Firm in the Labor and Employment practice and co-leader of the Technology, Media, and Telecommunications ("TMT") strategic industry group, based in Epstein Becker Green's New York office.

Ian Carleton Schaefer
Member of the Firm
New York Office
ischaefer@ebglaw.com
212/351-4787

5 Employment Law Considerations in 'The Cloud'

Introduction

What is "the cloud," and what on Earth (pun intended) does cloud computing have to do with employment law?

While many definitions abound, cloud computing at its core is a form of remote electronic data storage, processing, and application services that are hosted over the Internet. For data, instead of storing information on a computer or server at an office or place of business, it is stored in "the cloud." As an emerging and disruptive technology, the cloud is a collection of larger servers located elsewhere (e.g., data centers) and maintained by a vendor. The data or application becomes accessible to users anywhere there is an Internet connection. If you've ever used webmail or TurboTax, for example, you've operated in the cloud.

Whether your company utilizes public, private, or community-based clouds, and whether the delivery model is Software as a Service ("SaaS"), Platform as a Service ("PaaS"), or Infrastructure as a Service ("IaaS"), cloud computing offers companies the ability to quickly deploy on-demand platforms and analytical applications. Cloud computing provides organizations with tremendous cost and logistical advantages, in addition to creating real value-add through agility and collaboration.

And while cloud computing is not new per se, the speed and scale with which these platforms can be utilized has accelerated dramatically in recent years. According to recent reports, more than half of U.S. businesses now use cloud computing and will spend more than $13 billion this year on cloud computing and managed hosting services. The pace of utilization and investment are projected to rise dramatically in the coming years.

While the jurisprudence in this area is still in its nascent stage, CEOs, CIOs, General Counsels, and HR executives looking to stay ahead of the curve would be well-served to check the forecast – to leverage the power of the cloud, while considering the employment-law implications noted below.

1. **Solving Rainy Day Problems While It's Only Partly Cloudy: Wage and Hour Concerns** [1]

Wage and hour lawsuits are heating up across the U.S. Often brought as class or collective actions, the number of these lawsuits has increased by 350 percent since 2002. Governmental crackdowns on misclassification are also trending. Indeed, President Obama's fiscal 2015 budget allocates $11.8 billion in discretionary funding to the Department of Labor, including a $41 million increase to the Wage-Hour division, to ensure workers receive appropriate wages and overtime pay.

As wage and hour lawsuits and governmental audits become more pervasive, employers face new challenges, particularly as technologies change the way people work. The advent and proliferation of cloud computing – allowing the ability to work more flexibly, and outside of the traditional office setting – has transformed the landscape for employees. As a result, the cloud has also ushered in new legal and financial challenges for employers.

Off-the-clock work for non-exempt employees is a particularly troubling issue with cloud computing. Employees who are not exempt from overtime pay must be paid for all work performed, whether in the office, at home, or commuting – a "suffer or permit" standard as the Fair Labor Standards Act instructs. As company storage of emails and documents in the cloud becomes more pervasive, coupled with the use of smartphones and remote access work, the line between "working hours" and "non-working hours" has blurred substantially. And the following situations are likely more real-life than hypothetical.

For instance, a non-exempt employee who can access work email through a smartphone would need to be paid for each email she reads outside the office. As a result, some employers have banned non-exempt employees from downloading or accessing work email through a smartphone, to prevent wage-hour troubles. Even without a smartphone, however, many employees feel a need to log-on to their email through remote access or webmail to check-in. For example, if a boss tends to work late, an administrative assistant may check his email after work to determine if he has to come in early the next morning, or to manage the influx of work the following day. Additionally, organizational and managerial norms may dictate a "24/7" workplace – or an "always available" expectation. While the ease of access in a cloud computing workplace is certainly valuable to the business, such ease can be a double-edged sword when it comes to properly compensating non-exempt employees.

To avoid a wage and hour action against your company, it is critical to monitor and track off-the-clock work to accurately compensate the worker – a challenging task for many employers. Most timekeeping by non-exempt employees is self-reported, either on a physical timesheet or timekeeping software. As employers seek to combat off-the-clock issues, they may need to resort to different methods to track time. A program that tracks the amount of time logged on to a remote access site would solve overtime concerns, but potentially raises privacy issues.

Establishing strict policies against off-the-clock work for non-exempt employees is a good first-step to circumvent wage and hour actions. However, if litigation arises, a judge will be more concerned with the number of hours actually worked and compensated, rather than

what the policy says – actions speak louder than words. Employers and managers of non-exempt employees need to train their employees on recording working hours and to set expectations about off-the-clock work.

EBG handles wage and hour actions in all industries. For more information about the latest developments and tips, check out our blog or download the Wage & Hour Guide app, available in the iTunes App Store.

2. PHI in the Cloud: HIPAA, Data Privacy, and Data Security [2]

Companies and their HR and benefits departments that utilize cloud platforms to store and access personnel records, benefits information, and the like are likely storing protected health information ("PHI"). The obligations and restrictions regarding PHI are governed by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The consequences for failure to comply can be severe to a company's bottom line.

In March 2013, the Department of Health and Human Services ("HHS") finalized the HIPAA Omnibus Rule, which expanded HIPAA's applicability beyond covered entities (health care providers, health plans, and health clearinghouses) to business associates. By definition, a "business associate" is a person or entity that creates, receives, maintains, or transmits PHI in fulfilling certain functions or activities for a HIPAA covered entity. The definition of a business associate includes a cloud service provider if it maintains PHI in a persistent manner. The cloud service provider is a business associate even if the agreement with the covered entity does not contemplate any access, or where access is only on a random or incidental basis. As such, both the covered entity and cloud service provider would be subject to the requirements under HIPAA.

Employers must be mindful of their requirements to remain compliant with HIPAA when storing PHI in the cloud. Employers that determine a cloud vendor is indeed a business associate must have a business associate agreement ("BAA") in place. The BAA sets the terms for what PHI is being maintained or processed by the cloud vendor and for knowing where the data goes, from inception to disposal.

In housing PHI in the cloud, covered entities and their business associates must adhere to the HIPAA Privacy and Security Rules. Neither covered entities nor business associates may use or disclose PHI, except where the Privacy Rule permits or requires. Covered entities and the business associates must also maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting PHI. With regards to the administrative safeguards, entities must perform a risk analysis to evaluate the likelihood and impact of risk to PHI. By storing PHI in the cloud, covered entities must ensure that cloud providers have physical and technical controls in place to safeguard PHI from unauthorized access, acquisition, use, and disclosure.

Employers need to be especially mindful of the risk of data breach, which can carry significant reputational harm and monetary liabilities. In the event of a breach, employers and their business associates must comply with HIPAA's breach notification rule (at 45 CFR §§ 164.400-414), which requires notification following a breach of unsecured PHI. A breach is generally an impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of the PHI. The breach notification rule provides three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was

made in good faith and within the scope of authority. The second exception applies to the inadvertent disclosure of PHI by a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate, or organized health care arrangement in which the covered entity participates. The final exception applies if the covered entity or business associate has a good faith belief that the unauthorized person to whom the impermissible disclosure was made would not have been able to retain the information. Following a breach, covered entities must provide notification of the breach to affected individuals, the Secretary of HHS, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

When moving to the cloud, employers should remain aware that while business associates are directly liable under HIPAA, covered entities may also be directly held responsible for any actions of their business associates if their business associates are acting as agents of the employers. Noncompliance with HIPAA can result in costly fines and penalties. The fines and penalties for a HIPAA violation range from $100 per violation with a maximum fine of $25,000 for repeat violations, to $50,000 per violation with a maximum fine of $1.5 million. Ultimately, subject to any indemnification within the BAA, covered entities are held responsible when it comes to monetary and reputational consequences; however, both a covered entity and business associate assume responsibility under recent revisions to the HIPAA rules.

Employers using cloud-based platforms should do their due diligence as covered entities throughout the vendor selection process. Employers must make continuous efforts to ensure that the integrity, confidentiality, and availability of PHI are consistent with federal standards.

3. The Cloud, the Evolving Role of the CIO, and the Increasing Importance of Attracting and Retaining Key IT Talent [3]

As technological advances increasingly transform and become more integral to the workplace and development of new business, consideration must be given to ensuring that an employer has highly-skilled executives and IT employees in place to design and implement the right technologies for the business. In the 17th Annual Global CEO Survey by Price Waterhouse Coopers (2014), 86 percent of CEOs surveyed noted that technological advances will transform their business over the next five years. Companies surveyed concluded that no matter what their industry, they will need to think like technology companies. They will invest in “new digital ecosystems” to make digitization possible, in order to meet changing customer expectations to deliver products and services in a new way. Investment will be made in business analytics, socially enabled business processes, mobile customer engagement, cybersecurity, on-demand business and technology services, sensors, robotics, battery and power technologies, 3-D printing and wearable computing such as Google Glass and similar devices.

To lead the charge, many companies are looking to hire Chief Information Officers at the executive level, to oversee IT departments and collaborate with the business leaders to implement ready-made technologies and develop forward-thinking strategies. The role of the CIO will surpass that of the Chief Technology Officer, who traditionally has focused on the engineering aspects of developing new technology solutions. The decision to hire a CIO will require an assessment of actual needs, technological and customer experience trends, and the skills required to lead the organization’s business strategy in accordance with the projected business plans as well as those required to provide the necessary vision to propel

innovation.

Indeed, the job description for a CIO has been radically transformed in the cloud-based environment and has shaped corporate recruitment, retention, and compensation strategies. In today's market, a CIO need not only possess keen technological and information management expertise. Instead, the new CIO job description has expanded significantly, as companies are increasingly seeking CIOs with legal backgrounds, to deal with the highly regulated environment; financial management skills, to understand how their role impacts the bottom-line; enterprise data management skills, to make sense of the company's big data; people skills, to handle vendor-partner relationships; and IT security and compliance expertise related to the data privacy and security issues noted above.

As a result, businesses will need to develop new strategies to attract and retain CIOs, as well as other IT professionals, as they compete for highly-skilled employees in a market where the competition for highly-skilled talent is rising. Consideration should also be given to identifying those who can be trained and promoted from within the organization. Indeed, the role and relative importance of the CIO has and will continue to morph as organizations continue to invest in cloud technology, with the CIO at the center of driving organizational change and helping businesses transform, commanding a greater importance at the table.

In light of the increasingly important role of the CIO and IT professionals across industries, consider the following steps in attracting and retaining the right talent:

- Develop a clear job description with specific job duties, responsibilities, and reporting lines and identify the key skills and track record that the person should possess to fill the position.
- Determine a recruitment budget for executive search firms and/or assess in-house recruitment capabilities.
- Design a competitive salary and benefits package (including retirement and health insurance) for the position as well as competitive bonus, incentive, or deferred compensation programs, taking into account corporate culture, industry compensation statistics, geographical considerations, as well as experience-level required for the position.
- Determine whether an employment agreement will be required as part of the hiring process, as well as the scope of any non-compete, non-solicitation, restrictive covenants, confidentiality, or trade-secret agreements.
- Request and verify candidate references and consider the appropriate background checks and pre-employment screenings that will be required in accordance with applicable law prior to extending an offer of employment.
- Address timely compliance with any necessary U.S. immigration requirements if seeking highly-skilled foreign workers.

As advancements in technologies continue to shape businesses and customer expectations, recruitment and retention of key talent to address these needs must be a top priority. Further, consideration must be given to making appropriate hires as well as to developing strategies for training and promotion from within the organization. Moreover, once these key positions are filled, it will be imperative to ensure that competitive compensation programs are in place to retain the highly sought-after professionals that will become integral to the organization, all the while safeguarding the company's interests in the event that the

employment relationship with these key players comes to an end.

4. The Cloud Keeps Following Me: Jurisdictional Challenges [4]

The beauty and power of cloud computing is that a company's information is available wherever you are and whenever you need to access it. The upshot is that the data may not necessarily be located in a single place. Typically, a vendor will host the data in a physical location (in large data centers, in remote and secure locations) that may have no correlation with where the company otherwise conducts business. These servers housing your data can move for various reasons, such as if the servers outgrow their physical space or if the vendor relocates for business purposes.

While these logistical happenings may have little impact your company's day-to-day use of the server, such changes have the potential to pose challenges should litigation arise. While we are not aware of any filed cases on the topic as of the date of this publication, jurisdiction is always an important factor to consider when running your business. The geographical location of an employer's data can potentially expose employers, for litigation purposes, to jurisdiction in a state or country where they do not want or expect to be "doing business." The executive suite and chief legal counsels spend considerable time strategizing how to avoid "doing business" in certain jurisdictions based on laws that may not be favorable. So how is an employer to prevent the location of their data in the cloud from broaching unwanted jurisdictions, subjecting them to lawsuits, far from their backyard?

One best practice is to draft the vendor contract to protect the company's interests. The vendor contract can be written to include both choice of law and choice of forum clauses, to dictate where and under what law any disputes will be resolved – and not based on the vendor's location. Also, as part of any vendor contract, it is important to ensure that the vendor cannot move your data/server before giving sufficient notice. If the vendor plans to move to a state in which you don't want to potentially be subject to suit, the vendor needs to give the employer sufficient time to find a new host in a more favorable location. You may wish to consider a contract that specifically limits the states or countries where data may be stored, to avoid surprise transfers.

In some cases, multiple vendors may be used at a single time. Different offices may host data through local vendors. A single office may use more than one data hosting vendor to handle different data, based on department, client, or project. When data is hosted by various vendors, it's essential to establish each contract to protect the company's jurisdictional presence and to stay on top of any changes with the vendor.

Additionally, the location of the data in the cloud, including a company's choice in a vendor based on the location of servers, may have privacy implications. While the U.S. does not have federal laws limiting the transfer of personal data (HIPAA covers the transfer of health information, as discussed herein), other countries have much stricter data privacy laws. The European Union Data Protection Directive prohibits the transfer of private data across national borders without an adequate level of protection. As U.S. federal law does not have the requisite level of protection, as defined by the Directive, if individual American companies want to store and transfer data between the U.S. and the EU, they must enter into a Safe Harbor. For example, if a Swiss company's personnel files are kept in the home office, a Human Resources representative in New York may not be able to reach an employee's file absent a Safe Harbor agreement. Additional challenges may arise when employers are forced to timely respond to subpoenas when the information sought is located in a

jurisdiction that places restrictions on the transfer of personnel files or other personal data.

Companies should take stock of where they currently do business, and add jurisdictional exposure to the list of considerations in moving data to the cloud.

5. **Working from the Cloud: Managing an Agile Workforce (Beyond Telecommuting)** [5]

Recent studies estimate that nearly 20 to 30 million Americans work from home at least one day per week. In fact, telecommuting in the United States grew by 73 percent from 2005 to 2011. By 2016, an estimated 63 million people will work from home in the United States.

One of the more powerful and natural byproducts of the cloud is its impact on the nature of work. And in many ways, moving toward cloud-based storage models will have the likely long-term effect of fundamentally redefining the workplace – adding momentum to the trend toward building an agile workforce that is attached not to brick and mortar - but to laptops and smartphones. Managing an agile workforce in the cloud will be a nuanced challenge for employers going forward.

With flexible work arrangements on the rise because of its noteworthy benefits (which studies have shown can lead to increased employee engagement, motivation, and satisfaction), it is ever-more important that companies develop and maintain guidelines to manage this agile workforce. Prior to establishing alternative working arrangements, a company should conduct a careful evaluation of its organizational needs, along with a clear description of employee roles, to assess which roles may be appropriately identified as appropriate for a flexible working arrangement status. The following guiding principles should also be considered by employers in managing their agile workers:

- Develop a protocol for agile workers, and train and educate employees and managers. Organizations should clearly identify standards for teleworking, so that everyone involved understands what flexible working arrangements are available and can set expectations accordingly. Training should include topics such as:
    - teleworking processes and procedures;
    - compliance with applicable company policies (including those regarding confidentiality and privacy);
    - safety in the alternative workplace; and
    - communication with the office.
- Stay in tune. All team members should be aware of the expected lines of communication, as well as the organization’s acceptable response time.
- Manage by results. Define clear organizational objectives and closely monitor those objectives to ensure that the organization’s expectations are being met. In the event the flexible arrangement becomes viewed as a right and not a privilege, or is abused internally, reassess whether the arrangement makes sense for the organization.
- Make work status clear. Use instant messenger, shared calendars, and out of office messages to keep team members aware of each other’s work availability.
- Document the arrangement. An agreement between the employee and employer that

outlines the flexible working arrangement, including its terms and requirements, is a useful way to set expectations and manage the relationship. All such agreements should reiterate the at-will nature of employment (where applicable) and should confirm the circumstances under which the employer may terminate the arrangement.

- Develop a trusting work environment. Micromanaging day-to-day activities of employees may be detrimental to overall productivity and may foster an environment of distrust. Use agreed-upon and objective performance indicators as a means to build trust between managers and telecommuting employees.

In addition to implementing management guidelines, there are legal risks to consider prior to instituting an agile worker policy:

- Employer Property: If employees are using the organization's property, such as smartphones or laptops, have them sign documents acknowledging receipt. Additionally, employers should require employees to take action if the equipment is damaged or stolen, and indicate who is responsible for replacing such equipment.
- Other Costs: If telecommuting employees will pay for their home equipment, Internet service, electricity, and/or other relevant expenses, the parties should be clear on this point. Note that prior to establishing rules in this regard, employers should review applicable law on expense reimbursement.
- Data Security: In an effort to ensure data security, employers should require teleworkers to use a VPN or secured connection while remotely accessing company data. This measure can help safeguard confidential or sensitive information being accessed by teleworkers. Employees should also reiterate their agreement to comply with confidentiality and other similar agreements.
- Taxation Issues: Employees who work from a home location that is in a different state than their assigned office may be subject to different tax treatment and withholdings. Payroll departments should be placed on alert to handle appropriate deductions and withholdings issues for agile workers. Further, employers should be mindful that, when permitting employees to telework from alternative workplaces in states where the company does not already do business, the taxing authorities in such states may deem the company to be "doing business" in that state. As a result, the employer may need to register to do business in that state and pay corporate taxes there.
- Jurisdictional Issues: As previously noted herein, permitting an employee or employees to work in a location in which the company doesn't otherwise do business may subject it to suit in an unfamiliar (or unfriendly) state.
- Workers' Compensation: To limit potential liability for injuries at the home office, employers should clearly define teleworkers' hours and work space. For example, employers can require employees to designate a specific area of the home to serve as an office, and deem 9 a.m. to 5 p.m. as working time. Although such a designation may not preclude all unexpected liability, it may help to limit same.
- Wage Hour Concerns: As previously discussed, employers considering agile working arrangements should clearly track employee hours, to ensure their accuracy, and make sure that non-exempt employees are being compensated in accordance with the Fair Labor Standards Act.

The Technology, Media, and Telecommunications strategic industry group can assist in navigating employers through the panoply of issues and strategic initiatives noted above.

Contributor Credits:

[1], [4] These sections were prepared by Nancy L. Gunzenhauser, an Associate in the Labor and Employment practice, in the New York office of Epstein Becker Green.

[2] This section was prepared by Marshall E. Jackson Jr. and Brandon C. Ge. Both are Associates in the Health Care and Life Sciences practice, in the Washington, DC, office of Epstein Becker Green.

[3] This section was prepared by Michelle Capezza, a Member of the Firm in Employee Benefits and Health Care and Life Sciences practices, in the New York office of Epstein Becker Green, and co-leader of the Technology, Media, and Telecommunications strategic industry group.

[5] This section was prepared by Ian Carleton Schaefer, a Member of the Firm in the Labor and Employment practice, in the New York office of Epstein Becker Green, and co-leader of the Technology, Media, and Telecommunications strategic industry group. Gregg Settembrino, a Paralegal (not admitted to the practice of law) in the firm's New York office, also contributed to the preparation of this section.

Technology, Media, and Telecommunications Strategic Industry Group

The Technology, Media, and Telecommunications strategic industry group of Epstein Becker Green's Labor and Employment practice is comprised of a team of attorneys who advise technology, media, and telecommunications companies—public and private, large and small—regarding workplace management, employee benefits, immigration, litigation, and business matters affecting their organizations. Members of the Technology, Media, and Telecommunications strategic industry group have extensive experience as both in-house and external counsel in handling day-to-day and bet-the-company matters in this space.

About Epstein Becker Green

Epstein Becker & Green, P.C., founded in 1973, is a national law firm with approximately 250 lawyers practicing in 10 offices, in Baltimore, Boston, Chicago, Houston, Los Angeles, New York, Newark, San Francisco, Stamford, and Washington, D.C. The firm is uncompromising in its pursuit of legal excellence and client service in its areas of practice: Health Care and Life Sciences, Labor and Employment, Litigation, Corporate Services, and Employee Benefits. Epstein Becker Green was founded to serve the health care industry and has been at the forefront of health care legal developments since 1973. The firm is also proud to be a trusted advisor to clients in the financial services, retail, and hospitality industries, among others, representing entities from startups to Fortune 100 companies. Our commitment to these practices and industries reflects the founders' belief in focused proficiency paired with seasoned experience. Visit www.ebglaw.com

LinkedIn **@ebglaw** **RSS** — ***Follow Epstein Becker Green***
