*Maryam Nabiyeva**

# The High Price to Pay for the Cloud: How Cloud Based Storage Applications Streamline Data Storage, but Pose Legal Issues and Security Risks to Private Sector Employers and Employees Alike

***Abstract***

*The advent of new cloud-based technologies has generated questions and concerns over their application in the workplace. While everyday users store mounds of information in the cloud without realizing it, businesses specifically chose cloud-storage for convenience and in a lot of cases necessity. This however may open them up to liability beyond that of "data breaches." While the courts in United States has addressed this issue in the realm of privacy concerns to public employees (i.e. government employees), private sector employees and employers alike are left in the dark as to their obligations and liabilities.*

*This article will discuss generally what cloud-computing is, what legal issues it poses in the areas of wage and hour law, intellectual property law and general privacy considerations for both the employer and employee alike. It will also examine whether necessity exists for employers to safeguard utilization of cloud based storage in the workplace, if they chose to store protected health information, and the likelihood of impending necessity to re-draft employment agreements to protect work product and other privileged client information that may be stored in the cloud. This article will also look at any existing or proposed legislation and review any cases on the issue that have been decided in the country, that could help both sides in navigating the ever advancing world of cloud computing. Finally, this article attempts to propose adequate solutions where legislation and the courts have failed.*

***Annotasiya***

*"Cloud" əsaslı texnologiyaların inkişafı özü ilə birlikdə bu texnologiyanın iş mühitində tətbiqi ilə bağlı suallar və problemlər meydana gətirdi. Gündəlik istifadəçilər səbəbini dərk etmədən xeyli informasiya saxladıqları halda, bizneslə məşğul olanlar cloud-bazalardan sırf rahatlığına və bir sıra əhəmiyyətli məsələlərə görə istifadə edirlər. Lakin belə istifadə nəticədə onları "məlumat pozuntuları" üçün məsuliyyətlə üzbəüz qoyur. ABŞ məhkəmələri bu məsələyə dövlət işçilərinin şəxsiliyinin pozulması çərçivəsində baxdığından özəl sektor işçilərinin və işəgötürənlərinin oxşar öhdəlik və məsuliyyətləri məqamı qaranlıq qaldı.*

*Məqalədə ümumiyyətlə "cloud" kompyuterçiliyin nə olduğu, əmək haqqı və iş vaxtı, əqli mülkiyyət hüququ və həm işçi, həm də işəgötürənlər üçün ümumi şəxsilik baxımından*

* Maurice A. Deane School of Law at Hofstra University, Juris Doctor Candidate.

*hansı hüquqi məsələləri meydana çıxardığı müzakirə edilir. Məqalədə eləcə də, hər iki tərəfə inkişafda olan "cloud" kompyuterçilik dünyasında manevr etməyə yardımçı olmaq üçün mövcud və ya təklif olunmuş qanunvericilik və qəbul edilmiş hər hansı bir məhkəmə işinin olub olmaması araşdırılmışdır. Nəhayət, məqalədə qanunvericilik və məhkəmələrin uğursuz olduğu məsələlər üzrə adekvat həllər təklif edilməyə çalışılır.*

## Contents



## Introduction

Gone are the days of storing important papers in boxes spread out all over the office. Gone are the days of contracting with an outside vendor to come and pick up the boxes of papers and transport them to a secure off site storage. Nowadays, even though employers still contract with third parties, they do so in order to store their data and documents in the cloud, by purchasing "infrastructure platforms" and not physical storage space.[1] Storage has gone form a warehouse space to a fictitious but all to real space in the cloud.[2] As of 2013, majority of U.S. businesses were utilizing some sort of cloud storage.[3] The phrase can be heard in every office, however not everyone understands exactly what it means, and very few comprehend the implications its use has in the workplace.[4] If you tell an everyday employee that the cloud is a "collection of larger servers located elsewhere

[1] Samara Lynn, *20 Top Cloud Services for Small Businesses*, (Dec. 11, 2012), http://www.pcmag.com/article2/0,2817,2361500,00.asp.

[2] *Id.*

[3] Reuven Cohen, *The Cloud Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing*, Forbes (Apr. 2013), http://www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-u-s-businesses-now-use-cloud-computing/. (last visited Oct. 22, 2015).

[4] Toby Merrill, *Cloud Computing: is Your Company Weighing Both Benefits & Risks?* ACE Group, (Apr. 2014), http://www.acegroup.com/us-en/assets/privacy-network-security-cloud-computing-is-your-company-weighing-both-benefits-risks.pdf. (last visited Oct. 22, 2015).

and maintained by a vendor," he or she may look at you with a blank stare.[5] This is because it is a fairly new technology, and businesses are still learning to navigate their way through the cloud, even though its advent can be traced back to the 1960s.[6] Nowadays, any business from construction companies to Information Technology providers and law firms are more than likely to utilize some kind of cloud applications.[7] On may ask: 'what exactly is the cloud? And where is it? And what does it have to do with private sector employment?'

This note will discuss in detail what cloud-computing is, what legal issues it poses in the areas of wage and hour law, employee and employer privacy considerations, necessity for employers to safeguard their application if they chose to store protected health information in the cloud, and the likelihood of impending necessity to re-draft employment agreements to protect work product and other privileged client information that may be stored in the cloud.[8] This paper will start with a discussion on how employers and employees utilize public cloud applications in the workplace, primarily focusing on mid to bigger sized companies with varied employee pool: part time, full time etc. The paper will then focus on the specific issues that arise when employers use cloud based applications in the workplace are employee privacy issues, such as possible breach of Computer Fraud and Abuse Act, as well as possibility of trade secret theft, wage and hour violations and possible Health Insurance Portability and Accountability Act (HIPAA) violations.[9] The first half of the paper will delve into what cloud computing is and how employers chose to utilized it.[10] The last section will offer possible solutions that employers and employees alike can agree on in the workplace, as well as discussion on what actions the legislature could implement to find a uniform solution.[11]

---

[5] Ian Schaefer, *5 Employment Law Considerations When Cloud Computing*, Law 360, (Apr. 8, 2015), http://www.law360.com/articles/523645/5-employment-law-considerations-when-cloud-ccomputingcomputing. (last visited Oct. 22, 2015).

[6] Arif Mohamed, *A History of Cloud Computing*, Computer Weekly (Mar. 2009), http://www.computerweekly.com/feature/A-history-of-cloud-computing. (last visited Oct. 22, 2015).

[7] Cohen, *supra* note 3.

[8] *Id.* Since So many businesses are choosing to move to the cloud, a revolution in employee-employer relationship is on the way. Robert Milligan, *Neglect of Cloud Computing Policies In Workplace Can Provide Perfect Storm for Trade Secret Theft*, TRADE SECRETS LAW (Oct. 10, 2013), http://www.tradesecretslaw.com/2013/10/articles/trade-secrets/neglect-of-cloud-computing-policies-in-workplace-can-provide-perfect-storm-for-trade-secret-theft/

[9] Schaeffer *supra* note 5.

[10] *See* discussion *infra* part II.

[11] *See* discussion *infra* Part VII.

# I. The basics of cloud applications

Chances are, we all have used cloud applications recently. If you used Gmail or DropBox, you have been utilizing cloud applications.[12] For a lot of businesses, cloud computing is a useful, emerging tool that seemingly makes data and information storage an easier task for any business.[13] It allows for a large bandwidth, which means more information can be stored at a lower cost to businesses.[14] Simply put, cloud computing allows a user to store, and subsequently have access to data and information over the internet, through a third party vendor, as opposed to a computer's hard drive.[15] A very important aspect of cloud computing to note, is the absence of a hard drive, a tangible area where information is stored.[16] The beauty of cloud applications is that you can potentially work from anywhere, be it on the beach, on your couch or in your office building, just on a different floor.[17] The possibilities of mobility are limitless.

What a lot of people don't understand is that the term "cloud computing" encompasses a lot more than what their perceptions of the definition are: it is a term that "doesn't describe a single thing – rather it is a general term that sits over a variety of services from Infrastructure as a Service at the base, through Platform as a Service as a development tool and through Software as a Service replacing on-premise applications."[18] Complications arise when one tries to discern what exactly cloud-based application is. Let us now break the terms down.

There are three categories of cloud storage: private, public and hybrid.[19] The most common would be a consumer cloud service, which would be labeled public, an example of which is your run of the mill email providers: Gmail, Yahoo, Outlook etc., as well as services such as Box.com, DropBox, and Google Drive.[20] These services would be utilized to simply store information a user may need to access on a different device, in a different place.[21] In this instance, a user is utilizing an Internet based application to

[12] Schaefer, *supra* note 5.
[13] Merill, *supra* note 3.
[14] Schaefer, *supra* note 5.
[15] Eric Griffith, *What is Cloud Computing*? (Apr. 2015), http://www.pcmag.com/article2/0,2817,2372163,00.asp. (last visited Oct. 22, 2015).
[16] *Id*.
[17] *Id.*
[18] Ben Keeps, *Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS*, http://www.rackspace.com/knowledge_center/whitepaper/understanding-the-cloud-computing-stack-saas-paas-iaas (Last updated, October 22, 2013).
[19] *Id.*
[20] Merrill, *supra* note 4.
[21] *Id.*

store information.[22] The way a company with cloud needs would utilize cloud storage is similar to how a consumer would, by simply picking one that would meet the company's needs and start using it.[23] However, an employer would have to chose a cloud storage service carefully, and consider a lot more than an individual consumer would, like security, possibility of breach, storage needs and cost.[24]

## A. Cloud in the workplace

When it comes to businesses utilizing cloud applications, there is a whole different world of cloud.[25] As mentioned earlier on, cloud computing's humble beginning was in the 1960s.[26] However, it did not become wildly popular or even user friendly until the late 1990s, with introduction of Salesforce, which delivered applications via a website.[27] With each redesign, a user was moving away from utilizing a computer's hard drive, and into an intangible space in the "cloud."[28] There are three types of business cloud computing applications: IaaS (infrastructure as service), PaaS (Platform as service) and SaaS (software as service).[29] The most commonly used cloud application by employers is SaaS: SaaS uses a third party vendor to manage the storage and delivery of information.[30] The concept is simple: a user would be able to access applications through the Internet.[31] An example of such application would be SalesForce, a client relationship management application (CRM) that provides personalized cloud storage services to businesses for a wide range of needs, such as client contact information and marketing and sales data.[32] A control of Software as Service application mostly lies in the cloud manager's hand, which is usually a third party vendor.[33] PaaS gives the user access to tools that are maintained by the cloud providers and that can be used to develop applications and to make those applications available to the user's customers.[34] The most likely demographic to use PaaS would be Software developers working on a development project, because PaaS is not ideal for large storage or portability

[22] Lynn, *supra* note 1.
[23] Virtela Blog, http://www.virtela.net/enterprise-vs-consumer-cloud/ (June 29, 2012).
[24] *Id*.
[25] Merrill, *supra* note 3, at 1.
[26] Mohamed, *supra* note 5.
[27] *Id.*
[28] *Id.*
[29] Lynn, *supra* note 1.
[30] Merrill, *supra* note 4.
[31] *Id*.
[32] Salesforce, http://www.salesforce.com/what-is-salesforce/?d=70130000000mA5n&internal=true (last visited Oct. 22, 2015).
[33] Merril, *supra* note 3, at 2.
[34] Keeps, *supra* note 9.

that businesses may require.[35] When utilizing IaaS, cloud buyers rent space in a virtual data center from an IaaS provider.[36] Rather than purchasing servers, software, datacenter space or network equipment, clients instead buy those resources as a fully outsourced service on demand.[37] This would require businesses to outsource for cloud storage, and lead to inability for speedy access to the stored data, which is not desirable for companies wanting to conduct regular, uninterrupted business.[38]

When implemented and structured correctly, cloud computing storage posses numerous benefits to both employees and employers.[39] Availability of alternative ways of accessing and storing information provides more flexibility in the workplace, having more employees work remotely and eliminating offsite storage allows employers to scale down on office size and other expenses, thus allowing for higher salaries.[40] It expedites daily activities by allowing easy access to data, fosters collaboration between team members, no matter where they may be at the time, and it is a lot more cost effective than storing files off site.[41] Cloud computing is also a way to for companies' to save money in another way: it can cut companies' information technology costs by twenty percent or more.[42] Additionally, cloud computing can minimize time wasting behaviors as it providers for greater visibility for employers, albeit sometimes at the cost of employee privacy.[43] However, the flip side is that employees use personal devices at work or perform work related tasks off the clock.[44] Not only productivity, but also security of valuable information stored in the cloud may be at risk: public cloud environments are massive, providing hackers with a larger "attack

[35] *Id.*

[36] Profit Bricks, https://www.profitbricks.com/what-is-iaas (last visited Oct. 22, 2015).

[37] Keeps, *supra* note 9.

[38] *Id*.

[39] Jim Lynch, *What Are the Benefits and Drawbacks of Cloud Computing*, TECHSOUP, http://www.techsoup.org/support/articles-and-how-tos/what-are-the-benefits-and-drawbacks-of-cloud-computing. (last visited Oct. 22, 2015).
(Feb, 2015).

[40] *Id.*

[41] *See* Lynch *supra* note 39; *See also* Merrill, *supra* note 3 (stating that other benefits include reduced hardware needs, an environmentally friendly choice and advantage in the market).

[42] J. Nicholas Hoover, *Compliance in the Ether: Cloud Computing, Data Security and Business Regulation*, 8 J. BUS. & TECH. L.,255, 260. "These savings come from reduced deployment time, limited customization, the self-service nature of cloud services, the lack of up-front costs on technology infrastructure, and often simpler user interfaces that require less training." *Id.*

[43] *Id*.

[44] *See* Merrill, *supra* note 4; *see also* Hoover *supra* note 42 (stating that "the lack of control and transparency inherent in cloud computing opens up the risk that malicious employees working for the cloud provider could take possession of data to which they should not even have access.").

surface" to probe in comparison to private networks.[45] The mix up of devices and clouds can have a dangerous effect on privacy and confidentiality of business related information.[46]

## II. Misclassification of employees: wage and hour concerns

While the benefits of cloud applications give businesses a one up in the competitive market, and make operations cheaper and more efficient, employers may get caught up in cost effective aspects and overlook the basic but crucial concerns regarding wage and hour law.[47] How are the two subjects related? With the help of cloud storage, both employees and employers are "less tethered to their offices, homes, and even their physical computer systems than ever before."[48] Also, with proliferation of Bring Your Own Device (BYOD) polices, it becomes easier for employees to access work related files at lunch, and after hours especially if they are able to synch their devise with the work cloud.[49] This means more employees working from home, at their own pace, always connected, and always online, not necessarily punching in their hours.[50] With easy accessibility, comes the desire and need to answer emails at any time.

Under FLSA, "work not requested but suffered or permitted to be performed is work time that must be paid for by the employer."[51] An employee may feel the urge to answer his or her boss's emails at 1am, if they have access to it. With new legislation afoot from the Department of Labor, the minimum salary level for the "white collar" overtime exemption will more than double from the current level of $23,660, meaning that more than an estimated 5 million employees will suddenly require overtime pay for work done after hours.[52] Since 2000, "white collar" workers have been

[45] Lynch *supra* note 39.

[46] *Id.*

[47] *See* Schaefer, *supra* note 5.

[48] Journal of Internet Law, July 20, 2010.

[49] Patrick J. Beisell, Something Old and Something New: Balancing "Bring Your Own Device" to Work Programs with the Requirements of the National Labor Relations Act, 2014 U. Ill. J.L. Tech. & Policy 497, 501 (2014).

[50] Amy D. Cubbage, *Rethinking the 24/7 Response* (Sept. 2015), http://mcbrayeremploymentlaw.com/category/wage-and-hour/; *see also* see also Merrill *supra* note 4. "BYOD policies Bring Your Own Device, or BYOD, refers to the cost-effective and employee-friendly policies some companies have adopted, allowing employees to bring their own smartphones, tablets, and laptops to work, then use them to access privileged company information and applications." *Id*.

[51] US Department of Labor, Fact Sheet #22: Hours Worked Under the Fair Labor Standards Act (FLSA), http://www.dol.gov/whd/regs/compliance/whdfs22.pdf. (last visited Oct. 22, 2015).

[52] *Supra* note 50.

working longer hours, and one of the main reasons for this is the blurring of line between on the clock and off the clock thanks to advances in technology, like cloud computing.[53] Technological advances present a plethora of incentives for employees to telecommute.[54] While this may mean that those who typically could not enter the workforce (like working parents) will do so now, it also may present difficulty for employers to follow the FLSA regulations and comply with other wage and hour laws.[55] In recent years, the U.S. Government has been cracking down on employers who misclassify their employees and impending legislature allocates $41 million to Wage and Hour Division of the Department of Labor.[56] This means that cloud computing comes at a time where employers need to be vigilant in making sure their workers are paid for over time and paid the proper salaries for any work they do in the office and at home.

Issues with overtime pay and classifications do not only arise with regard to telecommuters. More often than not, issues like this arise with regards to employees who have access to work email and files from home and work on projects on their own time.[57] Non-exempt employees must be paid for any and all work done, regardless whether it is at home, office, on their way to home or to work, or on vacation.[58] The FLSA defines the term "employ" to include the words "suffer or permit to work."[59] Suffer or permit to work means that if an employer requires or allows employees to work they are employed and the time spent is probably hours worked.[60] This presents difficulty to employers, as it becomes hard to gage what hours the employee actually worked while out of the office.[61] Concerns regarding nonexempt employees who by law are eligible for overtime pay are more than likely to rise in these instances.[62] Department of Labor sets out regulations for overtime pay by stating, “an employer who requires or permits an employee to work overtime is generally required to pay the employee premium pay

[53] Ashley M. Rothe, *Blackberries and the Fair Labor Standards Act: Does A Wireless Ball and Chain Entitle White-Collar Workers to Overtime Compensation?* 54 St. Louis U. L.J. 709, 711 (2010).

[54] *See* Journal of Internet Law, *supra* note 48.

[55] Schaefer, *supra* note 5.

[56] *Id*.

[57] *Id*.

[58] *Id*.

[59] U.S. Department of Labor Fact Sheet #22, *supra* note 31.

[60] *Id*.

[61] Schaefer, *supra* note 5.

[62] Wages and Hours Worked: Minimum Wage and Overtime Pay, http://www.dol.gov/compliance/guide/minwage.htm, *see also* U.S. Department of Labor Fact Sheet #23: Overtime pay requirement of the FLSA, http://www.dol.gov/whd/regs/compliance/whdfs23.pdf.

for such overtime work."[63] FLSA then provides additional explanations for who is considered an exempt and non-exempt employee.[64] Minimum and maximum wage (and subsequently overtime pay provisions) according to FLSA do not apply to an exempt employee, which the act describes as "any employee employed in a bona fide executive, administrative, or professional capacity (including any employee employed in the capacity of academic administrative personnel or teacher in elementary or secondary schools), or in the capacity of outside salesman."[65] FLSA goes on to define a lot more professions as exempt from its minimum wage and overtime provisions, and DOL sets out commonly used exemptions.[66]

For the purpose of this paper, attention should be drawn to the first exemptions set out in §213, referring to any person employed in a bona fide executive, administrative or professional capacity.[67] A definition of "professional capacity" could mean anything. A boss trying to avoid paying its workers for overtime hours for work done from home, may write a job description in such a way that would warrant one in understanding that his employee works in a "professional capacity" and thus is exempt from FLSA's requirement for overtime pay. However, FLSA will not likely allow an employer to get away with prescribing an administrative assistant or office manager with job duties akin to professional capacity.[68] Going off this standard, it becomes obvious that an employee must have advanced education and work in some sort of intellectual capacity, or as a scientist, to warrant being considered an exempt employee.[69] Or an employer may turn to another definition in FLSA referring to "Administrative Exemptions" under which an employee would be as non-exempt if certain conditions are met: 1) the employee must be compensated on a salary or fee basis (as

[63] U.S. Department of Labor Fact Sheet #23: Overtime pay requirement of the FLSA, http://www.dol.gov/whd/regs/compliance/whdfs23.pdf.

[64] 29 U.S. Code § 213 (2006).

[65] *Id*.

[66] U.S. Department of Labor, Fair Labor Standards Fact Advisor, http://webapps.dol.gov/elaws/whd/flsa/screen75.asp (last visited Oct. 22, 2015).

[67] 29 U.S. Code § 213.

[68] *See* U.S. Department of Labor, Fact Sheet #17D: Exemptions for Professional Employees Under the Fair Labor Standards Act (FLSA), http://www.dol.gov/whd/overtime/fs17d_professional.pdf (stating that the employee must be compensated on a salary or fee basis at a rate not less than $455 per week; the employee's primary duty must be the performance of work requiring advanced knowledge, defined as work which is predominantly intellectual in character and which includes work requiring the consistent exercise of discretion and judgment; the advanced knowledge must be in a field of science or learning; and the advanced knowledge must be customarily acquired by a prolonged course of specialized intellectual instruction).

[69] *See id*. (Explaining further that teachers, lawyers and medical professionals "holding a valid license or certificate permitting the practice of law or medicine is exempt if the employee is actually engaged in such a practice").

defined in the regulations) at a rate not less than $455 per week; 2) the employee's primary duty must be the performance of office or non-manual work directly related to the management or general business operations of the employer or the employer's customers; and 3) the employee's primary duty includes the exercise of discretion and independent judgment with respect to matters of significance.[70] Another option for employers, according to DOL, would be to pay its workers over $100,000, even administrative and secretarial staff.[71] The DOL worksheet provides that:

> Highly compensated employees performing office or non-manual work and paid total annual compensation of $100,000 or more (which must include at least $455 per week paid on a salary or fee basis) are exempt from the FLSA if they customarily and regularly perform at least one of the duties of an exempt executive, administrative or professional employee identified in the standard tests for exemption.[72]

However, it's not likely that a lot of employers will be willing or able to proportionally raise its employees' salaries to start at $100,000. So what will happen to businesses that will try to cut corners with their employee classifications to avoid paying overtime? Wage and hour concerns have always been a hot button issue for unions, employees, and the government and even more so recently.[73] With businesses moving to cloud-based applications, employees are becoming more and more connected to the office and spending more hours from home on work related matters.[74] However, they may not necessarily see the hours they put in reflected on their pay stubs.[75] Should they raise the issues, they may be told that they are exempt, hence are not eligible for overtime pay.[76] Employers need to be cautious in properly classifying employees, and especially with regards to accurately compensating them for work done, since wage and hour lawsuits and governmental audits are becoming more and more prevalent.[77]

---

[70] U.S. Department of Labor, Fact Sheet #17C: Exemption for Professional Employees Under the Fair Labor Standards Act (FLSA), http://www.dol.gov/whd/overtime/fs17c_administrative.pdf. (last visited Oct. 22, 2015).

[71] U.S. Department of Labor, Fact Sheet #17H: Highly-Compensated Workers and the Part 541-Exemptions Under the Fair Labor Standards Act (FLSA), http://www.dol.gov/whd/overtime/fs17h_highly_comp.pdf.

[72] *Id*.

[73] *See supra* note 5 (stating that "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 nonexempt employees").

[74] *Id*.

[75] Workplace Fairness, *Overtime Exemptions*, http://www.workplacefairness.org/overtime-exemptions

[76] *See* Schaeffer *supra* note 5.

[77] *Id*.

The way some employers are actually handling issues arising with cloud accessibility and overtime pay and trying to avoid possible lawsuits is by banning nonexempt employees from being able to have access to work email through any sort of device outside of the office, whether through mobile devices or otherwise.[78] However, while employers may institute work policy prohibiting utilizing work laptops at home or downloading apps that will allow them to remotely access their email on their phones, there are still ways for employees to access their work email through web-based email.[79] For example the ability to log into email from the employer's portal at home, presents a flexible opportunity to finish up work not complete during the day.[80] Many companies have this option, and there is not really a way to stop an employee from logging in.[81] This is just one of the ways cloud based applications are blurring the lines between on the clock and off the clock.[82] One thing is clear, cloud based applications make the workplace more accessible outside the office.[83] This leads non-exempt employees to put in more hours whether willfully or because the office culture demands so.[84] What the employers will do to stay in line with FLSA requirements remains to be seen.

## III. Employee privacy concerns

Perhaps one of the most talked about and litigated issues in the employment sector, without even considering the role cloud computing may play, is the issue of employee privacy.[85] Employers are known to monitor activities of their employees in various ways, including scanning sent and received e-mails by anti-virus and anti-spam software, tracking a worker's every keystroke and mouse click, monitoring communications via remote computing platforms, storing copies of e-mail messages sent and received on servers where individual workers cannot access or delete the messages, logging information on actions performed by workers, including the applications used and the files accessed and printed, monitoring internet access, online sessions, electronic chat conversations, and remotely viewing what the worker is doing in real time.[86] Nearly 80 percent of large employers

[78] *Id*.

[79] *Id*.

[80] *Id*.

[81] *See* Roth, *supra* note 46.

[82] *Id*.

[83] *Id*.

[84] *Id.*

[85] *See* Schaefer, *supra* note 5.

[86] Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States,* 26 Berkeley Tech. L.J. 979, at 981-82 (2011).

listened to employee phone conversations and voicemails, read electronic files and e-mails.[87] While an employer may not necessarily engage in all those monitoring activities, employers do utilize one or many of the ways to monitor their staff.[88] Employers monitor their employees for three reasons: "protecting information and other intellectual property assets; increasing productivity; and avoiding liability."[89]

Once it becomes clear what employers do to monitor their employees, the second question that arises is whether or not that infringes on employee privacy rights. To answer that, we first have to look at the sources of those rights.[90] For public employees that determination is easy: The U.S. Constitution provides for civil rights of individuals against actions of state actors, i.e., state and federal governments, including government employers.[91] No such rights exist for private sector employees.[92] Private sector employers' practice of monitoring their employees' electronic transactions has raised questions about the appropriate balance between employees' privacy rights in the workplace and companies' rights to protect themselves and their employees by monitoring their employees' electronic transactions.[93] Instead, private employee rights are derived from common law and are divided into four categories: (1) intrusion upon seclusion; (2) public disclosure of embarrassing private facts; (3) publicity which places a person in a false light in the public eye; and (4) commercial appropriation of a person's name or likeness.[94] Although the rights are derived from two different sources, the approach to figuring out whether or not an employee is entitled to those rights is the same.[95] The main question to be answered by courts remains the same: does the employee have a reasonable expectation to privacy? [96]

While there has been a plethora of legal disputes regarding employee privacy in the workplace, application of law currently governing such matters is not as clear-cut when it comes to the use of cloud computing at

[87] Justin Conforti, *Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the Ortega Test in Quon v. Arch Wireless*, 5 Seton Hall Circuit Rev. 461, at 462.

[88] Determann & Sprague, *supra* note 60 at 982.

[89] *Id*. at 982.

[90] *Id*. at 986.

[91] *Id*.

[92] Gregory T. Alvarez and Jason E. Ruff, *Private-Sector Employees and Workplace Privacy in the Electronic Era*, N.J. Lawyer Magazine, 247 N.J. Law. 24 (August 2007).

[93] UNITED STATES GENERAL ACCOUNTING OFFICE, COMPUTER-USE MONITORING PRACTICES AND POLICIES OF SELECTED COMPANIES 1 (2002), http://www.gao.gov/assets/240/235595.pdf.

[94] Determan & Sprague, *supra* note 79, at 986.

[95] *Id*.

[96] *Id*.

work.[97] Legal disputes as to what type of privacy rights employees have in the workplace have been developing over the past few decades.[98] However the most prominent of these lawsuits have generally revolved around public sector employees. Courts have held that under the Fourth Amendment, public employees have a reasonable expectation of privacy in the workplace.[99] However, employees in the private workforce currently enjoy no privacy in their electronic mail communications, and hence no privacy in what and how they utilize cloud based applications the workplace.[100]

First however, it is important to lay down the rules of privacy that Courts have found to apply to public employees, so we can understand the issues of privacy in the private sector as well. In the landmark case on this issue, *O'Connor v. Ortega*, the court set out a two prong tests to determine the extent of privacy in the workplace.[101] The court stated that in order to figure out if the employer's conduct is justified, two questions had to be answered: 1) whether an employee has reasonable expectations of privacy and 2) whether employer's intrusion was justified.[102] *Ortega* case involved a physician who worked at a state hospital and was responsible for training psychiatry residents.[103] The hospital officials became concerned about possible misconducts by him of the program, including but not limited to charges of sexual harassment against him by a female student and hospital employees and inappropriate disciplinary action against a resident.[104] While he was on administrative leave and an investigation of the charges against him was pending, the hospital officials, allegedly, in order to take inventory searched his office and seized personal items from his desk and file cabinets that were used in administrative proceedings resulting in his discharge.[105] The physician filed charges against the hospital, claiming that the search violated his Fourth Amendment rights.[106]

In answering the two questions posed, the court first discussed the context under which the expectation of privacy should be reasonable stating that

---

[97] Ilana R. Kattan, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617 (2011).

[98] Journal of Internet Law, *supra* note 31.

[99] O'Connor v. Ortega, 480 U.S. 709, 718 (1987); see also Leventhal v. Knapek, 266 F.3d 64,78 (2d Cir. 2001) (holding that "employee had reasonable expectation of privacy in his office computer but agency possessed individualized suspicion justifying search").

[100] Todd M. Wesche, *Reading Your Every Keystroke: Protecting Employee E-Mail Privacy*, 1 J. High Tech. L. 101 (2002).

[101] Ortega, 480 U.S. 709, at 726.

[102] *Id*.

[103] *Id*.

[104] *Id*.

[105] *Id.* at 709.

[106] *Id.*

"workplace includes those areas and items that are related to work and are generally within the employer's control."[107] The court held that "respondent had a reasonable expectation of privacy in his office."[108] In discussing the reason behind the decision, the court stated:

> Dr. Ortega did not share his desk or file cabinets with any other employees. Dr. Ortega had occupied the office for 17 years and he kept materials in his office, which included personal correspondence, medical files, correspondence from private patients unconnected to the Hospital, personal financial records, teaching aids and notes, and personal gifts and mementos.[109]

Turning to the second prong, the court discussed what constituted a reasonable intrusion.[110] The court ultimately remanded the case stating "public employer intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstance."[111] It was left for the Court of Appeals to determine whether the conduct was reasonable.[112]

Years later, the Supreme Court applied the test set out in *Ortega* in a case where a city police officer brought an action against city, police department and police chief alleging that police department's review of officer's text messages violated Fourth Amendment.[113] The court held that the city's review of text messages was reasonable, and thus, did not violate the Fourteenth Amendment.[114] First, the court found that indeed Plaintiff had a reasonable expectation to privacy in the content of his text messages.[115] However, under the second Ortega prong, the Supreme Court held that "the search was justified at its inception because there were reasonable grounds for suspecting that the search [was] necessary for a non-investigatory work-related purpose."[116]

Even though the Plaintiff in *Quon* was a public employee, the Supreme Court touched on areas of privacy that are relevant to private employees as well, and especially to the topic at hand.[117] The court however also cautioned itself stating that it "must proceed with care when considering the whole

[107] *Id*. at 716.
[108] *Id*. at 709.
[109] *Id*. at 719.
[110] *Id*.
[111] *Id*. at 725.
[112] *Id*.
[113] City of Ontario, Cal. v. Quon, 560 U.S. 746, 746 (2010).
[114] *Id*. at 765.
[115] *Id*.
[116] *Id*. at 761.
[117] *Id*. at 758.

concept of privacy expectations in communications made on electronic equipment owned by a government employer."[118] The court's concern was mainly that judicial interpretations and rulings on matters of fairly new technology, like cloud computing and text messaging, and their implications on privacy in the workplace should be approached with the utmost care, because the societal implications of those matters have not yet become clear.[119] The court wisely noted that changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.[120]

After analyzing the two judicial approaches to employee privacy (keeping in mind that both deal with public employees), we next dive into another possible source of privacy protection for private employees.[121] Since private employees are granted no statutory federal protection, there are alternatives that may offer some relief: the Stored Communications Act (SCA).[122] Congress enacted the Stored Communications Act as part of the Electronic Communications Privacy Act (ECPA) of 1986.[123] ECPA protects against various kinds of electronic surveillance and interception of communication by public and private actors.[124] There is one downfall of ECPA: the law does not protect against service provides, who also sometimes double as employers. [125]

SCA only applies to providers of an "electronic communication service" (ECS) and a "remote computing service" (RCS).[126] A provider of ECS allows its customers "to send or receive wire or electronic communications."[127] A provider of RCS supplies "computer storage or processing services by means of an electronic communication system."[128] The language of SCA prohibits "with the threat of fines and imprisonment: (1) intentionally accessing without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeding an authorization to access that facility; and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage

[118] *Id*.
[119] *Id*.
[120] *Id*. at 759.
[121] Conforti, *supra* note 61 at 465.
[122] *Id*. at 464.
[123] Kattan, *supra* note 70, at 628.
[124] Conforti, *supra* note 61, at 465.
[125] *Id*.
[126] *Id*.
[127] *Id*.
[128] RICHARD M. THOMPSON II & JARED P. COLE, STORED COMMC'N ACT: REFORM OF THE ELECTRONIC COMMC'N PRIVACY ACT (ECPA) (2015), https://www.fas.org/sgp/crs/misc/R44036.pdf.

in such system."[129] The beauty of SCA is that there are civil remedies available to those who feel their rights under SCA have been infringed upon.[130] To determine whether a communication is subject to protection under SCA we need to first characterize the cloud provider as either ECS or RCS.[131] This will help in determining what protections are allocated to communications maintained by a specific type of provider, by law.[132]

An ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications."[133] A provider that allows wire or electronic communications to be sent then is an ECS provider, in which case the SCA protects the communications, as long as the provider keeps the communication in electronic storage.[134] The question that arises with this definition is what exactly electronic storage is. Department of Justice (DOJ) defines it as communication that is "stored in the course of transmission by a service provider."[135] The term is also defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[136] There has been an ongoing disagreement between courts as to what types of communications are "stored in the course of transmission"; perhaps an unopened email would fit the bill.[137] However, there have been some major disagreements regarding this particular aspect of the definition as well.[138] So there are now two approaches to define what "stored in the course of transmission" means: the traditional approach as defined by DOJ and the new position taken by the Ninth Circuit, which holds that electronic storage applies to items even after they have been accessed.[139]

RCS is defined by the Act as "the provision to the public of computer storage or processing services by means of an electronic communications system.[140] An RCS provider, on the other hand offers computer storage or

[129] 18 U.S.C. § 2701 (1986).
[130] Determann & Sprague, *supra* note 60, at 982.
[131] Kattan, *supra* note 70, at 632.
[132] *Id*.
[133] 18 U.S.C. § 2510 (15).
[134] Kattan, *supra* note 70, at 632.
[135] *Id*. at 633.
[136] THOMPSON & COLE, *supra* note 97.
[137] *Id*.
[138] *See* Theofel v. Farey-Jone, 359 F.3d 1066 (9th Cir. 2004) (stating that emails left on a service provider's server after users downloaded them through their workplace email program could be considered stored for "backup purposes.").
[139] Cyber Telecom, http://www.cybertelecom.org/security/ecpacontent.htm (last visited Nov. 24, 2015).
[140] 18 U.S.C. §2711.

processing service to the public.[141] To qualify for the protection of communications stored by this type of provider, the communication must be "1) maintained on behalf of the RCS provider's customer and 2) solely for the purpose of providing storage or computer processing to the customer, such that the provider's authority to access the communication is limited to the extent necessary to provide storage or computer processing service."[142] An RCS provider to the public shall not knowingly disclose the contents of a communication, which is carried or maintained by that service.[143] Courts have held that private messages maintained on cloud based social media networking websites, such as Facebook and MySpace are maintained by an RCS provider.[144] RCS fits in perfectly with the definition of cloud computing. Under the definition, a service can only be a "remote computing service" if it is available "to the public"; services are available to the public if they are available to any member of the public who complies with the mandatory procedures and pays any required fees.[145] Even though cloud-computing falls nicely within the definition of RCS, it is not certain to what extent communications sent this way will receive warranted protection even under the SCA.[146]

Although a good idea, many consider that SCA "fails to provide a clear frameworks for understand whether a user has a reasonable expectation of privacy in his communications stored in the cloud."[147] Critics of SCA see it as failing to keep up with the emerging technology and communication tools.[148] Congress enacted SCA in the 1980s and has not amended the act to include protection for items stored using cloud software.[149] Besides the fact that the Act is outdated, there are also issues with the ESC and RCS defining what stored communications are.[150] For example, some courts have held that opened email messages stored for less than 180 days with an ECS Provider are subject to discovery.[151] The court reasoned that such emails were not in electronic storage.[152] Going a step further, the court noted that cloud based

[141] Kattan, *supra* note 70 at 636.
[142] 18 U.S.C. §2703(2)(b).
[143] 18 U.S.C. §2702(a).
[144] Crispin v. Christian Audigier, Inc., 717 F.Supp. 2d 965 (C.D. Cal. 2001)
[145] 18 U.S.C. 2711(2); *see also* Cyber Telecom, http://www.cybertelecom.org/security/ecpanutshell.htm#ecs.
[146] Kattan, *supra* note 70; *see also* Theofel, 359 F.3d at 1077 (leaving up to further interpretation the question of whether the rule set out in the case applies to cloud-based email system).
[147] Kattan, *supra* note 70, at 644.
[148] *Id*.
[149] *Id*.
[150] *Id*. at 636.
[151] United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009).
[152] *Id*.

email does not enjoy the same privacy protections as traditional email.[153] The DOJ also recognized that there is a limited protection to cloud based emails, and applications.[154] Hence, even though the SCA purports to offer some protection to the public in general, and private sector employees, it fails to do so adequately in the 21st century.[155]

There is also a tension between DOJ and the common law, one holding that opened emails are not considered to be stored on any provider and the other that protections should be granted as long as every other aspect of the definition is satisfied.[156] DOJ's approach favors the law enforcement by "conceptualizing the SCA not as protecting individual privacy, but as regulating how the government can obtain access to stored communications."[157] Even though the accent here is on the "government" one could easily imagine this playing out well in the workplace. An employer may likewise hold that web based emails that have already been opened are the property of the server provider, hence property of the employer, if the employer is also the server provider, which is often the case.[158] The fate of privacy in the workplace as it relates to cloud based applications and communications remains uncertain even with recent decisions.[159]

There have been attempts to increase workers' privacy through new legislation via 1993 Privacy for Consumers and Workers Act introduced in the Senate (PCWA).[160] The measure would have established a standard for notice, access to information, use limitations and would prevent abuses of electronic monitoring in the workplace.[161] The goal of the Act was to prevent abuses of electronic monitoring without prohibiting monitoring altogether.[162] Employers who violate the provisions of the PCWA can be subject to both civil penalties and private civil actions.[163] The Notice of Electronic Monitoring Act (NEMA) was also introduced in 2000; NEMA would have established a private right of action against employers who

[153] *Id.*; although the matter in that case is not one of work related access to emails, it is worth noting that the court 1) differentiated between web based and traditional email and 2) held in general that web based email should not be afforded privacy protection. *Id.*

[154] Kattan, supra note 70 at 635.

[155] *Id.*

[156] *Id.* at 644.

[157] *Id.*

[158] *Id.*

[159] *Id.* at 645.

[160] KRISTEN BELL DETIENNE & RICHARD FLYNT, AMERICAN BAR ASS'N., THE BOSSES' EYES AND EARS: THE PRIVACY FOR CONSUMERS AND WORKERS ACT (1996).

[161] Workplace Privacy, https://www.epic.org/privacy/workplace/, EPIC (last visited Nov. 23, 2015).

[162] DETIENNE & FLYNT, *supra* note 152.

[163] Workplace Privacy, *supra* note 153.

failed to give notice of wire or network monitoring.[164] Unfortunately neither one of the measures went any further. [165]

## IV. Employer privacy and trade secrets

On the other hand, cloud storage makes it easier for an employee to have access to sensitive top-level information on employer's cloud, information that may not be within the employee's duties to access.[166] This issue will arise most commonly when an employee is allowed to bring in their own device (or so called BYOD policy): laptop and cell phone.[167] For example, an employee may be backing up his or her work to Box.com, or Dropbox; in such an instance, if the user also has that same application on his or her mobile device, it means that the employee can take the information with them anywhere, whether they are on or off the clock.[168] This policy poses a great risk of security breach to employers and leaves them vulnerable to attacks.[169]

Moreover, former employees may still have access to the information after they leave the employers.[170] If this information is misused and a client is hurt in the process, employers will be subject to lawsuits by The Federal Trade Commission (FTC).[171] In the case of specific cloud based applications, like SalesForce, where company can store all of its client data, including contact information in the cloud, it is easy for an employee to have access to such

[164] *Id*.

[165] *Id*.; *See also The Privacy for Consumers and Workers Act: Hearing Before the Subcommitte on Employment and Productivity of the Committee on Labor and Human Resources*, 103rd Cong. 103-150 (1993), http://www.loc.gov/law/find/hearings/pdf/00161201005.pdf. The model Consumer Privacy Act set out possible ways to approach data collection: limiting access to personal data, collecting only data necessary for business purposes.

[166] Margaret Keane, *Clouds, Mobile Devices And The Workplace,* LAW 360 (Oct. 23, 2012), http://www.law360.com/articles/382923/clouds-mobile-devices-and-the-workplace.

[167] *Id*.

[168] *Id*. At that point, personal files and business files are inextricably intertwined, jeopardizing the employer's ability to protect its own information…

[169] *Id.*; *see also* Merrill *supra* note 4 (stating that "companies should consider the risk implications of allowing access to corporate data via employees' personal devices — devices over which the company exercises little or no control").

[170] Brian Krebs, *Data Theft Common By Departing Employees*, THE WASHINGTON POST (Feb. 26, 2009, 12:15pm), http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.html

[171] *See* Schaeffer, *supra* note 5; see also Federal Trade Commission, Complying With the FTCs' Health Breach Notification Rule, (Apr. 2010), https://www.ftc.gov/system/files/documents/plain-language/bus56-complying-ftcs-health-breach-notification-rule.pdf.

information at any time, anywhere.[172] This is exactly what happened in *F.T.C. v. Wyndham Worldwide Corp.* In that case the FTC sued a hotel chain for their system being hacked and all their client information being let out into the public.[173] Granted, the information was hacked by a third party, and not an employee, the hotel would have been in the same situation if an employee would simply access the customer information on their own time, having access to the company's cloud from home, or even having synched their device with the cloud of the workplace.[174]

Once an employee has access to employer's information and store it on a third party vendor's service, and then leaves or gets fired, the third party provider will be unlikely to cooperate in returning the potentially misappropriated information or trade secret to the employer.[175] Instead, they will argue that their obligation is to its "customer" which in the present instance would be the employee who created the account. [176] Since the cloud is basically "everywhere, by the time the issue gets resolved or not, the employee has had the information in his or her hand for a time now, and can pass it on freely. [177]

The type of information that an employee may have access to is limitless. It can be as basic but still sensitive, as client contact information, or it can be as advanced as a business merger agreement, or a new formula for a pharmaceutical drug.[178] Trade secrets are a hot issue at any workplace. With cloud storage, this issue becomes even more important because of how easy cloud storage makes it to access employer's information.[179] Companies that store trade-secret information in the cloud "face certain risks related to the use of a third-party provider, including (1) boilerplate terms of service that allow providers to access any information uploaded to the cloud and (2) rogue employees of the provider."[180] Employers typically require an employee to sign straightforward confidentiality agreements at the beginning of their employment.[181] Any employee that may come in contact with sensitive company information, by signing the agreement promises not

[172] Ben Kerschberg, Data Security And The Imperative of Private Clouds, Forbes (Sep. 9, 2011, 10:17am). http://www.forbes.com/sites/benkerschberg/2011/09/09/electronic-discovery-the-imperative-of-private-clouds/#24c2f109a003.

[173] FTC v. Wyndham, 10 F.Supp.3d 602 (2014).

[174] *Id.*

[175] Audra A. Dial and John . Moye, Trade Secrets in the cloud: Assessing and Mitigating the Risks. 17 J. Internet L. 1.

[176] *Id.*

[177] *Id.*

[178] *Id*.

[179] *Supra* note 164.

[180] http://apps.americanbar.org/litigation/committees/intellectual/articles/spring2014-0314-protecting-trade-secrets-stored-cloud.html.

[181] *Id.*

to divulge any of the information learned from his employer.[182] This means, do not tell anyone about X or Y that goes on in the workplace, the method used to come to the result etc.

When employees utilize cloud applications that enable them to store information and later access it to work on it from home, the line between the confidential agreement breach and simply doing their job becomes blurred.[183] That person is opening sensitive company information to breach by storing it on the cloud and then accessing it off the clock, in an area and over the network that may not be secured.[184] This in turn opens employee up to causes of action for breach of the confidentiality agreement, and opens employer up to causes of action for violating the Computer Fraud And Abuse Act (CFFA).[185] Abuse of CFFA creates a private right of action for anyone who suffers when another intentionally accesses a computer without authorization or exceeds authorized access and obtains information from a protected computer.[186]

In a recent Florida case, the court found that where an employee logged onto a work computer with valid credentials provided by the employer and emailed valuable documents from employer's computer to the employee's personal email address, a Computer Fraud and Abuse Act violation was maintained because the former employee continued to download the file after the employer revoked the authorization.[187] However, answering whether the employee had the right to access the employer's cloud, the court stated:

Nevertheless, PRLG's CFAA claim cannot survive the present summary judgment motion. As discussed above, there is no evidence before the court that Lynch accessed PRLG's cloud without authorization. Presumably, Lynch was authorized to access the firm's cloud shared drive while she was still working for PRLG. Other than Stone's allegation, which again lacks any indicia of personal knowledge, nothing in the record suggests that Lynch accessed the cloud after she left the firm. Even if Lynch intended to harm PRLG while using the shared drive to download materials while she worked for PRLG that alone would not establish that she acted "without authorization."[188]

Difficulties arise for employers when trying to prove that an employee accessed the cloud while no longer working for the employer, as stated by

[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] 18 U.S.C.A. § 1030 (West).
[187] Prop. Right L. Group v. Lynch, WL 242803 (D. Haw. May 30, 2014).
[188] *Id.* at *14.

the court above. [189] Once again, this is a great example of when the line gets blurred when employees can freely access the employers' cloud at any time, and it becomes problematic for the employer to then protect sensitive company information.[190] It seems that the courts are putting the burden of proof of employee's un-authorized access on the employer.

## V. Protected health information in the cloud and health information portability and accountability act violations

Employers may choose to utilize cloud services to store employee information in one place, including social security numbers, contact information (phone and address), benefit information, and other protected health information (PHI).[191] There is evidence suggesting that utilizing cloud applications to store PHI reduces compliance with HIPAA (Health Insurance Portability and Accountability Act).[192] Yet others state that the cloud is the safest way to store PHI.[193] While this is an efficient way of storing employee information that is easily accessible by the HR department, without proper safeguards it can be damaging not only to employee whose information may be stolen, but also to the employer's reputation and pocket.[194] Employers need to be mindful of the risks involved as well as the benefits, especially in regard to the risk of data breach, as there are laws set in place that employers have to follow if a breach happens.[195]

The Health Insurance Portability and Accountability Act of 1996 govern the obligations and restrictions regarding PHI.[196] As recently as 2013, U.S. Department of Health and Human Services finalized the HIPAA Omnibus Rule, which expanded HIPAA's applicability beyond covered entities (i.e., health care providers, health plans and health clearinghouses) to business

[189] *Id.*

[190] *See* Schaeffer, *supra* note 5.

[191] *Id.*

[192] Lee Bendekgey, Healthcare IT News (Sept. 4, 2013), http://www.healthcareitnews.com/blog/cloud-computing-reduces-hipaa-compliance-risk-managing-genomic-data.

[193] Scott Walters, *Why Protected Health Information (PHI) is Safer in the Cloud*, Executive Insight (Feb. 14, 2014), http://healthcare-executive-insight.advanceweb.com/Features/Articles/Why-Protected-Health-Information-PHI-is-Safer-in-the-Cloud.aspx

[194] *See* Schaeffer, *supra* note 5.

[195] *Id.*

[196] U.S. Department of Health & Human Services, Health Information Privacy, http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

associates.[197] The rule states:

> Individuals, organizations, and agencies that meet the definition of a covered entity under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information. If a covered entity engages a *business associate* to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information. *In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules*.[198]

A business associate is defined as anyone who:

> [O]n behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities…[199]

The Omnibus HIPAA Rule also revised the definition of business associates to expressly include particular entities, including many cloud service providers.[200]

---

[197] U.S. Department of Health & Human Services, Health Information Privacy, Covered Entities and Business Associates, http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html.

[198] *Id*.

[199] 45 C.F.R. 160.103; "

A definition of business associate includes Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. *Id*. The rule applies to any business associate that creates, receives, maintains, or transmits PHI while carrying out certain functions or activities for a HIPAA covered entity." *Id.*

[200] Frank Pasquale and Tara Adams Ragone, Protecting Health Privacy In An Era Of Big Data Processing And Cloud Computing, 17 Stan. Tech. L. Rev. 595 (2014). "It expressly includes "[a] Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information." *Id*.

Under this definition, a cloud service provider would be considered a business associate, and thus will need to follow the HIPAA rules.[201] Covered entities, on the other hand, must make sure that cloud providers have physical and technical controls to safeguard PHI from unauthorized access.[202] Employers in turn must make sure that they stay compliant with HIPAA when storing PHI in the cloud. An employer that utilizes a cloud provider for storing PHI must label the cloud provider as a business associate under the definition.[203] If that is the case, the employer must have a business associate agreement in place.[204] The difficulty lies in whether or not the employer will be willing, or able, to label cloud service provider as a business associate.[205] The agreement must set out what type of PHI is being stored, for how long, and give a detailed explanation of where the data is going, from the moment it is being stored to the moment it will no longer be in the cloud.[206]

Both covered entities and their business associates must adhere to HIPAA privacy and Security Rules. Neither party can use or disclose the stored PHI except where permitted.[207] This is reassuring to those whose PHI is being stored (like employees). However, employers must do their part and be mindful that data breaches are something that happens too often.[208] Employers must take appropriate administrative, technical and physical safeguards to ensure that PHI is protected. In other words, an employer cannot just leave it up to the cloud provider to ensure that the PHI is being safely stored, even if it is the cloud provider's job.[209] Employer bears the responsibility of ensuring that certain processes are in place to further protect the sensitive information.[210]

Where employer does not comply with rules and regulations set out by HIPAA in order to protect PHI, both employer and business associates may be held liable.[211] In an event of a breach, HIPAA requires compliance with its Breach Notification Rule, to affected individuals, Secretary of Health and

[201] *See* Schaeffer supra note 5.

[202] *Id.*

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] *Id.*

[207] Pasquale and Ragone, *supra* note 168. HIPAA Rule makes business associates directly liable for compliance with certain of the HIPAA Privacy and Security Rule. *Id.*

[208] *See* Schaeffer *supra* note 5.

[209] *Id.*

[210] *Id.* Among the types of things that covered entities must do is "to perform a risk analysis to evaluate the likelihood and impact of risk to PHI." *Id.*

[211] *Id.* A breach is an impermissible use or disclosure that compromises the security of the PHI. *Id.*

Human Services, and depending on the situation, to the media.[212] Noncompliance with HIPAA can result in fines and penalties, ranging from $50,000 to $1.5 million per violation.[213] Additionally, in 2014 FTC made an administrative ruling stating that it had authority to bring data security actions against HIPAA covered entities.[214] This means that FTC now has authority to intervene where PHI is compromised by entities.[215] This will surely make the employer companies who are utilizing cloud providers to store PHI to pay more attention and to ensure that their business associate agreements set out terms and guidelines that prevent such breaches in the future.[216]

## VI. Cloud applications and the future: proposed solutions

With each passing year, corporations and other private employers, are utilizing cloud computing for business needs.[217] While the benefits of switching to cloud computing are numerous, an employer must weight the pros and cons when it comes to legal aspects, especially those that concern employees.[218] Unfortunately, when it comes to a solution that can help avoid the issues that cloud based applications bring into the workplace there is no one size fits all.[219] Cloud based applications are a very intricate system that need a lot of fine-tuning and attention in order to work properly. Overprotecting it will strip it of its benefits and under-protecting it will cause chaos and myriad of legal issues.[220] Moreover, there is not one single cloud application that will fit the business needs of all the companies, so cloud storage and its use needs to be tailored to a particular need of a company and

[212] Pasquale and Ragone, *supra* note 168.
[213] *See* Schaeffer *supra* note 5.
[214] Bloomberg BNA, *FTC Affirms Data Security Enforcement Authority in Rejecting LabMd Arguments*, (Jan. 27, 2014) http://www.bna.com/ftc-affirms-data-n17179881620/.
[215] Christine Kern, FTC Takes Watchdog Stance Over Patient Data Encryption Standards, Health IT Outcomes (Jan. 25, 2016), http://www.healthitoutcomes.com/doc/ftc-takes-watchdog-stance-over-patient-encryption-standards-0001.
[216] *Id*.
[217] Pasquale and Ragone, *supra* note 168.
[218] *See* Diego Rosenfeld, *Five Things To Consider When Moving to The Cloud,* Boston Business Journal (Jan. 24, 2016, 1:00am), http://www.bizjournals.com/boston/feature/5-things/2016/01/five-things-to-consider-when-moving-to-the-cloud.html; see also Schaeffer *supra* note 5.
[219] Vince Deluca, Cloud Battles Intensify – It's No Longer 'One Size Fits All', CorpMagazine (Jul. 17, 2014), http://www.corpmagazine.com/technology/cloud-battles-intensify-its-no-longer-one-size-fits-all/
[220] *See* Kerschberg *supra* note 164.

the type of work being done by its employees.[221] To protect their information in general, it is in the employer's (or any business' for that matter) best interest to take reasonable steps to ensure that a cloud service provider has only as much access to company information stored in the cloud as is necessary, and that both the company and provider are doing everything possible to maintain the information's secrecy.[222] A solution that will be the most constructive and has a chance in satisfying all parties involved, will require for everyone to be actively involved (depending on the situation): employers, employees and the cloud service providers.[223] The most important and basic step that an employer needs to take is to choose the cloud provider very carefully, and has a detailed agreement in place to protect themselves and their employees.[224]

## A. Wage and Hour

The go-to idea that from a first look seems to solve all issues of utilizing cloud applications in the workplace, is to have a thorough employment/confidentiality agreement that will set out all the dos and the don'ts for both the employee and the employer.[225] Unfortunately, we live in the real world, where it is unlikely that the employer will agree to give up some of their rights to monitor employers and employees.[226] The truth however, is that as more work enters cyberspace and virtual worlds, this will have a profound impact on the nature of work itself, not to mention the legal doctrines of labor and employment law, so a common ground needs to be reached.[227] Still, a good place to start is at the negotiation table. While an employment agreement may not solve all the problems, it will record in writing what the parties are worried about, their expectations and help avoid any disputes arising between employees and employers.[228] Moreover, since many employers already utilize an employment agreement, it will be easy to tailor it to a workplace that wants or has already moved to the cloud. After

[221] Sommer Figone, *One Cloud Does Not Fit All,* RAPIDSCALE (Jan. 22, 2015), https://rapidscale.net/one-cloud-fit/.

[222] http://apps.americanbar.org/litigation/committees/intellectual/articles/spring2014-0314-protecting-trade-secrets-stored-cloud.html

[223] Pasquale and Ragone *supra* note 168.

[224] Lorry Freifeld, Keeping Employee Information Safe In The Clouds, Training Magazine (Sept. 28, 2012), https://trainingmag.com/content/keeping-employee-information-safe-clouds.

[225] *See* Schaeffer, *supra* note 5.

[226] FIND.

[227] Miriam A. Cherry, *A Taxonomy of Virtual Work*, 45 Ga. L. Rev. 951 (2011). The article talks about virtual life games and selection of avatars, but the author ventures on further to mention that majority of workforce is now being done in the cloud, in the ether and that will have substantial effect on labor and employment law. *Id.*

[228] Richard Harroch, Forbes.

all, once a business moves to the cloud, there is no coming back, so the employment agreement will probably be used for years to come.

Employers need to be firm in communicating their policies when setting out the agreement.[229] First and foremost, an employee needs to understand their scope of employment, meaning what duties they will be assigned, whether they are hourly or salaried etc.[230] This may seem basic, but a lot of confusion regarding wage and hour lawsuits stem from employees and employers alike being on different pages regarding what type of responsibilities an employee has (and thus how he or she is classified for FLSA purposes).[231] Policies that can be implemented are ones that completely forbid answering emails or sending them within a particular time frame.[232] To be on top of the hours employees log, a thorough system of tracking should be implemented that keeps a record of employees' hours.[233] A software system can be utilized to do this, which can monitor and track the amount of time employee spends not only at work, but also the amount of time spent on off the clock project.[234] There are systems that track the amount of hours attorneys spend on a certain litigation matter, with a click of a button on a screen, a system begins to track the time being spent on a particular matter.[235] Same logic can be applied to tracking hours of those employees who have to finish up a project off the clock.[236]

Tracking employee hours will go hand in hand with policies regarding BYOD.[237] To avoid any sort of data breach, BYOD policies need to be avoided

[229] Mark H. Wittow and Daniel J. Buller, *Cloud Computing: Emerging legal Issues or Access to Data, Anywhere, Anytime*, 14 J. Internet L. 1 (Jul. 2010) (stating that the need for clear and consistent communication of policies, practices and capabilities is necessary).

[230] *See* Schaeffer *supra* note 5.

[231] *Id*.

[232] Cubbage, *supra* note 50 (discussing a similar policy that was implemented at a company and stating that "the company bans the sending and receiving of email from 10 p.m. to 6 a.m. on weekdays and all weekend. It does this, it says, to reduce employee stress by providing a safe harbor for employees to rest and not contemplate workplace communications.").

[233] *Id*.

[234] *Id*.; *see also* US Department of Labor. DOL website even offers a timesheet tracking app for mobile devise to make this easier. http://www.dol.gov/opa/media/press/whd/WHD20110686.htm.

[235] Jill Turner Lever, Grace A. Byrd, *Manage Your Risk: Five Critical Employment Issues*, 272 N.J. Law. 9, 11 (October 2011). The best approach is for employers to implement a policy prohibiting non-exempt employees from working off the clock without authorization, requiring employees to report all time worked, and lastly, paying for this time either at the regular rate or the overtime rate, as may be applicable. *Id.*

[236] *Id.*

[237] *See* Cubbage, *supra* note 50.

at all costs.[238] However, for certain type of work and employees, taking work home may be absolutely necessary.[239] Here too, the employer needs to be strict and come up with a uniform policy for each employee type.[240] If for example there are employees that need to work off the clock, and are authorized to do so, those are the only ones that can either bring their laptop in, or be assigned a work laptop, that is configured to work off the network of the employer only, and that tracks the hours automatically. These policies will help avoid FLSA violations, both when non exempt employees work over 40 hours and can prevent situations where employee claims they worked more than they actually did, or when employer refuses to pay overtime claiming that the hours were not actually put in.[241]

## B. Employee Privacy

While public employees may enjoy a certain expectation of privacy, as it stands right now, private employees do not enjoy the same.[242] Unions and employee advocacy groups have been complaining about electronic monitoring for a few decades now, arguing that such practice are an invasion of privacy and "cause work related stress and low morale, and can be used in an unfair manner."[243] The status of privacy protection laws for private employees is ambiguous at best.[244] While there is no statutory relief as of yet, all is not lost for a private employee or the employer. When it comes to privacy, employees may choose to bring a common law action for conversion against employers. While this is more of a "right of ownership" question, it does fit well with certain documents that may be stored on the cloud, whether related to work or not.[245] In *Thyroff v. Nationwide Mut. Ins. Co.*, an employee brought an action against employer claiming conversion of his business and personal information stored on computer hard drives of leased computer.[246] In answering whether or not conversion was an appropriate cause of action, the court stated:

> We believe that the tort of conversion must keep pace with the contemporary realities of widespread computer use. We therefore answer the certified question in the affirmative and hold that the type of data that Nationwide allegedly took possession of—electronic records

[238] French, et. al, *Current Status and Issues with BYOD*, Communications of the Association for Information Systems, at 192, http://aisel.aisnet.org/cgi/viewcontent.cgi?article=3819&context=cais.

[239] *Id*.

[240] *Id.*

[241] *Id.*

[242] Determann & Sprague, *supra* note 60 at 982.

[243] The Private Workplace and the Proposed Notice of Electronic Monitoring Act.

[244] *Id*. at 81

[245] Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272 (N.Y. 2007).

[246] *Id*. at 1272.

that were stored on a computer and were indistinguishable from printed document is subject to a claim of conversion in New York.[247]

The law is well settled on employee privacy when it comes to e-mails.[248] Regulations just need to catch up to the more current technological advances in the workplace, like cloud computing, as is evidenced from the lack of regulation on the subject.[249] Just like it took courts a while to ascertain the privacy issues with e-mail monitoring, courts are just now starting to see more and more issues arising out of cloud computing and social media applications.[250]

That is why bringing torts action for conversion will speed up the process and bring the courts' attention to privacy issues with cloud computing. The tort action is twofold: it will be a penalty for employers and it will also possibly draw the attention of legislature. When employers are faced with lawsuits over employee privacy, someone is bound to get the government involved. Perhaps then the legislature will heed the arising issues and amend or pass a new bill that encompasses not only emails, but also documents stored in cloud-based applications.[251] This is where step two comes in: the legislature could consider reintroducing bills like NEMA (Notice of Electronic Monitoring Act) and other bills, modified to include BYOD policies and cloud based applications. When it was introduced, the Act provided that:

An employer who intentionally, by any electronic means, reads, listens to or otherwise monitors any wire communication, oral communications or electronic communication of an employee, or otherwise e monitors the computer usage of an employee without first having provided the employee notice meeting the requirements of subjection (b) shall be liable to employee for relief…[252]

The Act then went into describing exactly what is required from the notice meeting, what the employer must notify the employee of and when.[253] The Act also provided for a relief in the form of civil action for actual damages (not less than $5000), punitive damages and attorneys' fees and any other relief the court determines to be appropriate.[254] As it was set out then, the Act certainly takes substantial measures to safeguard employee privacy by

[247] *Id*. at 1278.

[248] Todd M. Wesche, *Reading Your Every Keystroke: Protecting Employee E-Mail Privacy*, 1 J. HIGH TECH. L. 101 (2002).

[249] *Id*.

[250] *Id*.

[251] *Id*.

[252] H.R. 4908, Notice of Electronic Monitoring Act, 106th Congress (1990-2000)

[253] *Id*.

[254] *Id.*

requiring much from the employer and setting monetary damages. It's not a surprise that it did not pass since the Act on its face is very anti-employer.

Since issues of privacy related to technology in the workplace remain to be hot topics at the moment, re-introducing a new and improved NEMA will draw attention to deficiencies in the private sector that employees face, and with plethora of litigation behind this issue, perhaps this time around the legislature will be compelled to pass it. Of course NEMA would have to be revised to specifically include cloud based application used for business purposes of an employer by an employee, and set out the type of monitoring that is prohibited by an employer. To achieve this result, NEMA would have to be combined with Privacy for Consumers and Workers Act introduced in the Senate (PCWA), another legislation that failed to pass.[255] That measure, as stated earlier, would establish varies standards for: notice, access to information, use limitations and would also prevent abuses of electronic monitoring in the workplace.[256]

## C. Employer Privacy

Employers and employees definitely disagree on the degree and magnitude of employer monitoring of the employee.[257] A 1994 study found that 81% of Americans think that employers should not monitor employees, whereas 70% of workers think that electronic monitoring is very important in evaluating their workers.[258] Although about twenty years have passed since that survey, as the world is changing and technology is taking over our lives, workplace more so than any other area, it's pretty certain that those number have not changed. This is certain from numerous litigations stemming out of issues of privacy in the public and the private sector employment alike.[259]

Employer privacy concerns as they relate to the use of technology in the workplace are closely related to employee privacy. If a policy or a law that is implemented favors the employee more, then employer may suffer by way of losing control over employee time, work product, inappropriate use of internet and the privacy concerning their clients.[260] However, if an employer oriented policy is implemented, the opposite happens: employees lose all and any privacy expectations and morale.[261] There are however policies that

[255] *Supra* Discussion Part IV.

[256] *Supra* Discussion Part IV.

[257] David Neil King, *Privacy Issues in the Private-Sector Workplace: Protection From Electronic Surveillance and the Emerging Privacy Gap*, 67 S. Cal. L. Rev. 441(1994).

[258] *Id*.

[259] *See* Discussion *supra* part IV

[260] Gregory M. Huckabee & Cherry Kolb, *Privacy in the Workplace, Fact or Fiction, and the Value of an Authorized Use Policy (Au*p), 59 S.D. L. REV. 35 (2014).

[261] *Id.*

could be structured in such a way that the two "opposing" sides will be able to balance out their interests and the privacy concerns of both the employee and the employer will be protected. Technically, their privacy issues are derived out of different concerns: employers want to protect their business interests and employees want to protect their personal space.

While majority of issues revolve around employee privacy, it is worth to note that employers are just as vulnerable.[262] Cloud services' distributed, Internet-based nature leaves the services open for attack and may put companies using cloud services at risk of being held legally responsible for losses of information.[263] A recent survey showed that about thirty six percent of employers have policies that address the use of public cloud storage services.[264] Employers, who value the privacy of their information, can ban the use of such cloud applications as Box, Dropbox or Google Drive and build one that is highly secured and requires access only in the office.[265] One logical step for an employer would be to implement such policy, and spend the money on building a secure cloud based storage application. This is surely time and money consuming, but a very important solution. If an employer possesses sensitive client data and depends on safety and privacy, this will be worth the effort. Building a thorough and bulletproof cloud storage application, that is managed in house (meaning no 3rd party can have access to "manage" it), will allow employer to then also prohibit BYOD devices (by implementing a "NO BYOD" policy, to be precise). Having a secure cloud means nothing if an employee can bring in his or her own device, and then store privileged information on it and leave. Along with (or instead of) a "NO BYOD" policy, an employer can go further and implement a strict policy that covers a broad range of concerns. A policy would need cover at least the following areas: 1) cloud based application is to be utilized for business purposes only; 2) BYOD devices are not allowed; 3) company reserves the right to monitor cloud activity of an employee; 4) set out disciplinary steps to be taken if the policy is violated.

Overall, access to cloud based applications in the workplace should be treated as employer property, just as any company issues laptop or cellphone would be. With this, employer should regulate such access by implementing policies concerning the use of such devices, just like they would regulate laptops and cellphones.[266] This is another area that can partially be mended

[262] *See supra* discussion Part V.

[263] *Supra* note 40.

[264] *See* Keane, *supra* note 137.

[265] *See id*. (Stating that certain companies, such as IBM has recently banned the use of Box and Dropbox).

[266] Privacy Rights Clearinghouse, Fact Sheet 40, 2014. https://www.privacyrights.org/bring-your-own-device-risks#3b byod employee responsibilities. For example, "as a security measure, employers often require employees who store company information on their

by way of a thorough employment contract that outlines employer privacy in regards to work product, client information and the use of cloud storage on and off the clock. This will alleviate any unexpected conflict with employees and set out ground rules for privacy from the get go. This is the area where it becomes more obvious that implementing policies that regulate employer privacy interests do not necessarily hinder regulations that protect employee privacy.

## D. PHI and HIPAA Compliance

Cloud computing has the ability to make everyone's job easier in the workplace: employees, employers and Health Insurance Providers (or third-party administrators). For employers, utilizing a cloud-based application to store this information means they have access to it on as needed basis without having to go through variety of systems and people.[267] If an employee has a question or concern or HR department needs to settle something quickly, accessing information off the cloud is much more time and money efficient than going through a third party. However, security concerns are even greater when it comes to storing PHI on the cloud; it is after all sensitive personal information at risk.[268]

One way employers can battle security breach is create their own cloud, meaning they will utilize a private cloud as opposed to a public one. This is a perfect solution for all security risk problems employers may face. As this will go hand in hand with solutions for employer privacy, the employers can kill two birds with one stone.[269] As employers have to remain compliant with HIPAA when storing PHI, employer will have more control over monitoring the cloud service provider, since the employer will technically be the provider.[270] This is the best solution to battle data security risks or leaving security matters to a third party.[271] Instead of ensuring that a cloud provider is adhering to HIPAA rules and then taking the fault when the contrary turns

personal devices to allow the employer to remotely delete data from the phone if the phone is lost or stolen. The same may be true when a person leaves the company." Other factors to be considered are: requirements to save and produce relevant information for legal purposes (e-discovery in particular) and consequences for deletion or alteration; processes for the end of an employment relationship and Trade secret policies and confidentiality agreements. *Id.*

[267] *See supra* discussion Part VI.

[268] *See supra* discussion Part VI.

[269] *See supra* discussion Part VII B.

[270] Lori Frefield, *Keeping Employee Information Safe in The Clouds: 3 steps to minimize risks of storing HR information and records in a cloud-computing environment,* TRAINING MAGAZINE (Sept. 2012), https://trainingmag.com/content/keeping-employee-information-safe-clouds. "Mitigate some of the risks of cloud computing by carefully selecting a vendor. Cloud vendors need to be thoroughly vetted based on factors such as the experience and technical expertise of personnel employed by the vendor."

[271] *See supra* Discussion Part VI.

out to be true, employer can navigate compliance issues themselves and mitigate any misconduct themselves.

Employers need to be very mindful of the risk of data breach, as their reputation and money is on the line. Legislature has gone through great steps to ensure that PHI is stored safely, as is evident from the hefty fines imposed for breach of HIPAA.[272] Thus, those employers that chose not to build their own private cloud will need to thoroughly research their cloud service provider. This is the most basic but very important step. The second step is to figure out if the provider is a business associate. If that is the case, they need to draft a thorough Business Associate Agreement.[273] This agreement needs to cover the type of information being stored, under what circumstances and who can have access to such information, the procedures to be followed in case of a breach, the safeguards that the cloud provider will put in place to ensure not only compliance with HIPAA but prevent the information from being hacked (like encryption), and what will happen to the data once the service agreement is terminated.[274]

## Conclusion

It is important to reiterate that there is no "one-solution-fits-all" approach when it comes to multi-dimensional issues with cloud-based applications in the workplace. That is to say, one set of policies will not necessarily fit to another company, as nature of business is different (doctors and accountants will most likely need cloud storage for different purposes). However, one policy, like a no BYOD policy or a thorough employment contract, can alleviate quite a few issues for a particular employer. This is what the private parties involved can do.

The Legislature can definitely get involved by passing laws that employers and employees alike will have to follow. As both the legislature and the courts speak on the matters of privacy, employers will be more compelled to implement policies that protect them from litigation. That will be one way to ensure compliance. When it comes to issues of PHI and other sensitive employee information, employers need to have bulletproof contracts set with cloud providers if they chose to go that route but the best solution remains to be designing and operating your own cloud based storage for all the needs of the employer. This will alleviate trade secret and privacy of employer's clients. It is also important for employers to implement and ensure compliance with all the necessary policies they set forth as to cover all their bases.

---

[272] *See supra* Discussion Part VI; *see supra* note 5.

[273] *See supra* Discussion Part VI.

[274] *See supra* Discussion Part VI.

A good starting point strategy, while it will require cooperation by both parties, is to draft a thorough employment contract that can outline all the concerns of employers. This has the potential to benefit all parties involved. While it may not be the best solution when it comes to employee privacy (this will have to be done through legislature), it can set out employers' expectations and let the employees know what they are getting themselves into. While it is clear that Cloud Based Storage Applications are becoming more and more prevalent in the workplace, both legislature and employees need to adjust to seeing more regulation of its use in the workplace, and employers need to adjust to properly implementing such regulations.[275] Whatever the risks cloud based technology provides to the workplace, one thing is sure: it promotes importance of key IT talent, meaning that it will open up a whole sector of employment for those who know the field well.[276]

[275] Dothang Truang, *How cloud computing enhances competitive advantages: A research model for small businesses*, ResearchGate, (January 2009), https://www.researchgate.net/publication/273447113_How_cloud_computing_enhances_competitive_advantages_A_research_model_for_small_businesses. "[Cloud computing] appears to be very beneficial for businesses, but at the same time it shows some challenges. Many businesses may see cloud computing as an inevitable means of success but some others may still hesitate in adopting it." *Id*.

[276] Schaeffer *supra* note 5.