

KEEP AN I ON THE SKY: E-DISCOVERY RISKS FORECASTED FOR APPLE'S ICLOUD

Daniel Carmeli*

INTRODUCTION

On February 22, and March 5, 1873, Barrett and Walton delivered to plaintiff ... one hundred and forty tierces of lard, to be shipped On the night of March 14, while the lard was stored in defendant's warehouse, awaiting shipment, it was destroyed by an accidental fire [S]aid goods put in said warehouse upon the agreement and understanding that the defendant should not be liable for a loss by accidental fire, was clearly made out. Such being the case, the common law liability is limited by this special agreement.¹

Some things have not changed since the fire of March 14, 1873. The competing interests of clients seeking convenient storage on one side against providers seeking protection from liability on the other continue to pervade the legal landscape. Naturally, some things have changed, such as the items being stored, the nature of the storage facilities, the associated risks, and the rules governing preservation obligations. Physical property has been replaced with electronically stored information ("ESI") and warehouses now take the form of remote data servers. And in addition to longstanding conventional risks, such as accidental fire, companies now face very particularized risks resulting from e-discovery obligations imposed by the Federal Rules of Civil Procedure.

Businesses have continuously attempted to reduce their exposure to e-discovery liability by utilizing risk-mitigating ESI storage systems. Cloud computing has emerged as a promising solution to reduce the risk of data loss as well as to transfer data loss liability to the vendor. Naturally, cloud computing service providers have expanded the limited liability provisions in their contracts to shield themselves and transfer the risk back to their clients. E-discovery has thereby perpetuated the age-old battle over the balance of risk.

This article illustrates how, despite cloud computing's theoretical advantages, the technology poses a variety of practical e-discovery risks for employers. Part I introduces cloud computing, plots out its inevitable integration into the workplace, and discusses its potential e-discovery advantages over conventional local data storage. Part II moves from the theoretical to the practical by applying a magnifying glass to Apple's new cloud computing product, iCloud, and revealing the various e-discovery risks that still remain. Finally, Part III offers employers some recommendations for how to reconcile their interest in cloud computing with the risks that the technology presents. While the right choice might be different for each business, the considerations and risks discussed below apply broadly.

I. THE ADVANTAGES AND LIKELY ADOPTION OF CLOUD COMPUTING IN THE WORKPLACE

A. *Meeting Demand for Increased Accessibility*

Accessibility to information and data has helped to drive the evolution of modern computing technology. From the personal computer itself² to diskettes, CDs,³ and flash drives,⁴ electronic storage devices have been invented and marketed to enable users to access their data from many discrete locations. The development of the Internet and remote storage also has made accessing digital information increasingly easier.⁵ In addition to spreading throughout consumer markets, these technologies have penetrated the workplace via unauthorized usage by employees⁶ as well as by enterprise-wide adoption by employers.⁷

Cloud computing has emerged as the next technology innovation for increasing data accessibility.⁸ Cloud computing is defined by the National Institute of Standards and Technology ("NIST") as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g.,

networks, servers, storage, applications, and services)⁹ that can be rapidly provisioned and released with minimal management effort or service provider interaction.”¹⁰ Essentially, cloud computing allows users to access electronic information remotely from any device with Internet access.

Cloud computing has already become familiar to consumers¹¹ and recently has been marketed heavily as the future of electronic data storage. On March 29, 2011, Amazon introduced its Cloud Drive, offering users a place to store their music in the cloud.¹² A month later, Google unveiled Music Beta by Google,¹³ adding music files¹⁴ to their portfolio of supported data types that can be uploaded and stored remotely.¹⁵ Finally, the much-anticipated Apple iCloud was released on October 14, 2011, providing Apple users with space in the cloud for multiple file types.¹⁶

Similar to the spread of CDs, flash drives, and the Internet discussed above, cloud computing has also made inroads into the workplace. Many organizations, including public entities,¹⁷ have responded with interest¹⁸ not just for the potential improvements in accessibility,¹⁹ but also to save money.²⁰ Some employers have already implemented cloud computing entity-wide.²¹ Other employers have expressed concern, however, by citing issues like security,²² data loss, performance, and loss of control.²³ In addition, employers and to a greater degree their attorneys, are concerned about the legal ramifications of cloud computing, especially in the context of e-discovery.

B. Cloud Computing and e-discovery

Cloud computing in its purest form, stores all ESI on a centralized remote server managed by a third-party service provider leaving no data on the local device itself.²⁴ Under this model, the integrity of an employer’s ESI is dependent not on the proper maintenance of an employee’s computing devices but rather on a remote server. As such, much of the responsibility is transferred from the employer’s agents, such as employees and IT staff, to the third-party vendor controlling the server. This shift helps employers comply with e-discovery preservation obligations and can often shield them from liability should they fail to do so.²⁵

1. E-discovery Duties Made Easier

i. ESI Destruction Less Likely

An organization’s duties to preserve ESI arise once it knows, or should know, that the ESI is relevant to impending²⁶ or reasonably anticipated litigation.²⁷ Employers must make sure not to “alter, modify, and destroy” such ESI.²⁸ Care and prudence are essential given employees’²⁹ knack for destroying such business data³⁰ through losing a flash drive with original payroll records³¹ causing a flash drive containing relevant files to fail,³² wiping out a laptop of a former employee adversarial party,³³ and continuing to use a laptop in a way that deletes data relevant to litigation.³⁴

Cloud computing can reduce the risk of data destruction by taking the ESI out of an employee’s hands and putting it into the cloud. It allows employers to entrust their data to individuals whose sole responsibility is to maintain the data’s integrity. Most employees likely do not prioritize the safekeeping of business files³⁵ but rather integrate it with other minor responsibilities. Even IT departments have numerous obligations in addition to monitoring employee storage and use of company files.³⁶ Using a third-party data storage vendor circumvents employee disinterest and cuts costs by reducing IT department workload.³⁷

Cloud computing also eliminates an incentive for employees to store data in additional locations. Employees routinely use portable data storage devices such as CDs and flash drives to transfer ESI between work and home computers.³⁸ They also commonly use cloud storage products,³⁹ such as email to download and access ESI on multiple devices.⁴⁰ However, cloud computing allows ESI to be accessed and modified while still remaining in the cloud, thus obviating the need for physical and electronic transfer methods. As a result, even employees who routinely fail to abide by a company’s data storage policies will no longer need additional storage devices or electronic transfer methods because all business documents will remain in the cloud.

Cloud computing even mitigates risks associated with portable devices such as smartphones, tablets, and laptops. Under a traditional decentralized paradigm, the consequences of losing or damaging such a device are

significant.⁴¹ With cloud computing, loss or damage to any and all devices is inconsequential because the ESI is located in the cloud.⁴² As such, cloud computing can help employers that have many employees handling multiple devices by reducing the risk of potential mismanagement of a single remote server or integrated system of servers.

ii. Reduce Scope of Reasonable Inquiry

Cloud computing also makes it easier for employers to certify that they have conducted the requisite “reasonable inquiry” for ESI during initial disclosures.⁴³ A court assesses the reasonableness of the inquiry based on the totality of the circumstances.⁴⁴ Factors considered include: “(1) the number and complexity of the issues; (2) the location, nature, number and availability of potentially relevant witnesses or documents; (3) the extent of past working relationships between the attorney and the client, particularly in related or similar litigation; and (4) the time available to conduct an investigation.”⁴⁵

Attorneys face the increasingly burdensome task of conducting a reasonable inquiry into their clients’ electronic data. First, most attorneys are not technology experts.⁴⁶ Second, electronic data storage has become increasingly complex and decentralized: “[P]otentially relevant information may be found in local and network computers, archive and backup data tapes, laptop computers, handheld storage devices (such as PDAs), cellular phones, voice mail systems and closed-circuit television monitoring systems.”⁴⁷ With so many potential locations for relevant data, “[t]he cost and complication of conducting discovery in a modern, distributed business computing environment can be enormous.”⁴⁸ Moreover, the courts have not been sympathetic. The courts commonly hold that parties who have availed themselves to the benefits of such technologies must also incur the associated discovery expenses.⁴⁹

Cloud computing mitigates these expenses because employers need to search only one location to find all of their ESI and satisfy the reasonable inquiry requirement. By having all ESI stored on one remote server, employers can satisfy the “location, nature, number and availability of potentially relevant ... documents” factor with a very limited inquiry. Searching in merely one location would be largely fruitless in the traditional decentralized storage model, but it is more likely to be deemed reasonable under a cloud computing system. This enables organizations that once expended considerable resources to scale down device use, as well as organizations that have always conducted limited inquiries to continue their practice.

2. Lower Risk of Employer Liability for Destroyed ESI

Unfortunately, as even the most casual computer user is aware, data has quite a propensity for getting itself deleted. In the realm of e-discovery, employers can face considerable liability for ESI destruction. Failure to preserve relevant documents could result in sanctions where the party in control of the data exhibits the requisite “culpable state of mind.”⁵⁰ Many courts have held that even mere negligence demonstrates sufficient culpability.⁵¹ Moreover, some have actually inferred negligence from the loss of relevant data.⁵² Therefore, it is not only prudent to reduce the risk of data destruction, but also to reduce the risk of liability in the event of destruction. Cloud computing may provide the appropriate solution.

By storing business data with third parties rather than on employees’ devices, employers reduce their liability by virtue of (1) their resulting lack of control over the cloud servers and (2) the likelihood for indemnification. An employer’s responsibility to preserve discoverable ESI is limited to that which is within its “possession, custody, or control.”⁵³ While courts have been split over whether “control” denotes a practical ability to obtain the data or a legal right to do so,⁵⁴ employers are generally deemed to have control over their employees’ work-related documents⁵⁵ as well as documents that are held by third-party data storage vendors⁵⁶ under either test.

Whereas employers may control the documents in either situation, the storage devices can be a whole different story. Employers are generally deemed to be in control of their employees’ local ESI storage devices,⁵⁷ but they would likely not be deemed in control of any cloud servers storing their ESI. The United States District Court for the Northern District of Illinois highlighted this distinction in *Grubb v. Board of Trustees of the University of Illinois*.⁵⁸ In that case, a leased laptop was wiped of its contents after it had been returned to the lessor. The court held that the user did not possess sufficient legal control over the returned laptop to warrant a duty to preserve.⁵⁹ The third party’s physical custody of the device made it liable for the loss. Companies might also find additional protection in the various jurisdictions that recognize an independent tort of spoliation against a third party.⁶⁰ Under

such a claim, a party seeking discovery could hold the third-party data storage vendor responsible rather than the employer.⁶¹

Moreover, even where an employer is deemed liable, it is more advantageous where the destruction is done by a third party rather than by an employee. An employer sanctioned for spoliation can seek indemnity⁶² from the individual or entity directly responsible for the destruction. Such indemnity claims are far more likely to succeed against a third party than against an employee. For example, in *Daynight, LLC v. Mobilight, Inc.*, the plaintiff won against the third-party defendant, KK Machinery, for willfully destroying laptops in its possession that contained data relevant to the litigation.⁶³ In contrast, sometimes employers cannot invoke indemnification against their employees.⁶⁴ Even where such indemnity suits are allowed,⁶⁵ they are rare and often fruitless given that employees generally have neither deep pockets nor indemnity insurance.⁶⁶

* * *

Cloud computing's potential risk-reducing advantages might seem to make it an easy sell for employers. However, as illustrated in the case study below, even a highly attractive cloud computing product can come with considerable risk.

II. iCloud IN THE WORKPLACE

On October 14, 2011, Apple released iCloud, its aptly named cloud computing service product.⁶⁷ Within only the first three days, twenty million people signed up for the service.⁶⁸ iCloud's immediate success, however, did not materialize overnight. Long before the recent buzz over cloud computing, Apple had already begun positioning itself to become a major cloud computing provider. The company had developed its brand on portable devices that increased access to ESI. Moreover, Apple had garnered a significant amount of consumer loyalty and retention. iCloud therefore entered the market with a considerable advantage.

However, the quality of a cloud computing service is not based solely on a provider's reputation. While cloud computing offers many potential advantages, its suitability often depends on the extent to which a particular storage plan meets a particular business's needs.⁶⁹ Even iCloud's Terms and Conditions agreement ("iTC") itself admits that "Apple ... make[s] no warranty that [] the service will meet your requirements."⁷⁰ This is particularly true for entities interested in reducing their e-discovery exposure. Entities that use iCloud as their exclusive data storage location would undermine their ESI's security, compromise their ability to comply with e-discovery obligations, and assume liability for data loss, even in the event of Apple's negligence. iCloud eliminates many e-discovery benefits of cloud computing and might not be the right choice for many businesses.

A. *iCloud as a Likely Choice for Employers*

1. Taking Advantage of Portability

The rise of data accessibility as discussed above, does not fully describe the technological boom of the past several decades. Strictly speaking, desktop computers make ESI very accessible: They have their own internal hard drives, USB ports for flash drives, CD drives for CD-ROMs, Ethernet ports for Internet connectivity, and operating systems to run software.⁷¹ However, desktop computer sales have been declining steadily for several years,⁷² a reflection of waning consumer interest in technologies that only make ESI accessible. Consumers increasingly demand technologies that also make ESI portable.⁷³ Such demand has for example, driven the evolution of the laptop to the lighter-weight tablet⁷⁴ and the cell phone to the more comprehensive smartphone.⁷⁵ Consumer demand is also a major element in the technological landscape that has set the stage for cloud computing.

Cloud computing follows in the footsteps of other notable Internet-driven enhancements to mobile computing. Just as wireless fidelity ("Wi-Fi") has made laptops much more useful,⁷⁶ mobile broadband has linked smartphone users to the Web,⁷⁷ and Internet connectivity has made the standard mp3 player a full multimedia experience,⁷⁸ cloud computing is similarly elevating data accessibility on portable devices.

Apple is well positioned to integrate cloud computing into its existing product line and market the resulting synergized technologies. Its suite of portable devices, which includes the iPod, iPhone, iPad, and laptop, provides employees the functionality to access and manipulate ESI⁷⁹ and engage in other work-related activities.⁸⁰ Moreover, all of these products have Internet connectivity,⁸¹ thereby enhancing the user's access to ESI.⁸² Apple's iCloud is unique among its competitors in that it takes advantage of a breadth and history of popular computing devices.⁸³

Unsurprisingly, Apple is not keeping this advantage a secret. When first released, the official iCloud webpage touted that the new product will “store[] your music, photos, apps, calendars, documents, and more. And wirelessly push[] them to **all your devices** – automatically.”⁸⁴ The emphasis on syncing devices was reemphasized further down the page:

iCloud is so much more than a hard drive in the sky. It's the effortless way to access just about everything on **all your devices**. iCloud stores your content so it's always accessible from **your iPad, iPhone, iPod touch, Mac, or PC**. It gives you instant access to your music, apps, latest photos, and more. And it keeps your email, contacts, and calendars up to date across **all your devices. No syncing required**. No management required. In fact, no anything required. iCloud does it all for you.⁸⁵

Moreover, for those interested in using their Apple devices for work, “iCloud automatically keeps your **documents** up to date across all your devices.”⁸⁶ By integrating cloud computing into a pre-existing line of popular portable devices, iCloud distinguishes itself as more than just remote storage. Rather, it integrates cloud computing into the familiar Apple mobile device experience.

2. Popularity Among Consumers and Employers

Apple's popularity among consumers and employers makes iCloud a particularly more likely and effective choice to achieve the full potential of cloud computing in the workplace. Apple has sold 250 million iPhones,⁸⁷ 84 million iPads,⁸⁸ and 60 million iPod Touches.⁸⁹ Moreover, as of April 2012, there were between 60–70 million Mac users.⁹⁰

While most of these sales have been to consumers, Apple has been marketing its products increasingly to corporations.⁹¹ The business community has responded favorably, with many companies purchasing them and distributing them to their employees.⁹² Fortune 500 companies have shown considerable interest: As of October 2011, 93% of Fortune 500 companies were testing or deploying iPhones⁹³ and 92% were testing or deploying iPads.⁹⁴ Small businesses have also shown high interest by purchasing 2 million iPads as of November 2010.⁹⁵ The iPad has penetrated a variety of industries, including healthcare,⁹⁶ hospitality, finance,⁹⁷ airlines,⁹⁸ food service,⁹⁹ wholesale/retail, communications, and energy.¹⁰⁰ This trend has been buttressed by high-profile sales to large corporations such as JPMorgan Chase,¹⁰¹ SmithBucklin,¹⁰² Mercedes-Benz Financial,¹⁰³ Wells Fargo, General Electric, Medtronic, and Hyatt Hotels and Resorts.¹⁰⁴

While some of these business-wide adoptions can be attributed to decisions made from the top down, popularity among consumers is also driving businesses to adopt Apple devices. This trend, an example of a phenomenon referred to as the “consumerization of IT,”¹⁰⁵ has gained speed over the last decade: Skype and LinkedIn have demonstrated how web-based communications and social networking, once marketed primarily to consumers, have made their way into businesses,¹⁰⁶ and cloud computing and cloud storage providers, such as Google Drive and Dropbox, respectively, have been particularly successful at penetrating the workplace.¹⁰⁷ But above all, personal computing devices, such as smartphones, laptops, USB drives, and now tablets (such as iPads), have consistently been crossing the divide.¹⁰⁸

Apple is perhaps best positioned to take advantage of this trend. The company has garnered considerable brand loyalty: Current Apple device owners tend to show higher interest in additional Apple products.¹⁰⁹ Those employees who already own Apple products for personal use are likely to want to use Apple products for business as well. As such, Apple, and particularly the iPad, has been hailed as “the king of the consumerization of IT,”¹¹⁰ “pushing the ‘consumerization of IT’ trend in a way that IT can’t stop.”¹¹¹

B. Is iCloud the Right Choice for Employers?

While Apple and its new cloud computing service, iCloud, might seem like a great sell on the surface, the apparently glossy image becomes far grainier under closer scrutiny. Unlike a pure cloud computing system, iCloud contains certain technological limitations that undermine its ability to assist employers to preserve their ESI and comply with e-discovery duties if litigation arises. Moreover, certain provisions within the iTC might actually leave employers with greater uncertainty, less control, and increased risk. Ultimately, iCloud might not meet employers' e-discovery needs.

1. Partial Mitigation of ESI Destruction and Liability Risk

Technologically, iCloud cannot guarantee that all of an employer's ESI will ultimately be stored on the cloud. Apple's overarching marketing pitch, that "iCloud stores your music, photos, documents, and more and wirelessly pushes them to all your devices. Automatic, effortless, and seamless -- it just works,"¹¹² does not tell the whole story. iCloud automatically updates a user's most recent ESI only onto devices that run iOS,¹¹³ such as iPads, iPods, and iPhones,¹¹⁴ and only when connected via a Wi-Fi network, as opposed to cellular service.¹¹⁵ Users with non-iOS devices, such as laptops and PCs, must manually access their documents on the iCloud storage website, download copies onto their local hard drives, and then upload the files back onto the iCloud storage website.¹¹⁶ This process downgrades iCloud from a cloud *computing* product to a cloud *storage* product.¹¹⁷ Although similar in name to "cloud computing," cloud storage is actually more akin to the traditional pre-cloud-based storage model, and creates the same e-discovery inconveniences.¹¹⁸ Like flash drives and CDs, iCloud for laptops and PCs leaves copies of ESI on both local and remote devices.¹¹⁹ With ESI scattered on employees' laptop and PC hard drives, complying with e-discovery preservation duties will remain a challenge.

In addition to considering the state of the technology, it is also important to assess the ramifications of the iCloud service contract.¹²⁰ Here, certain provisions in the iTC forewarn how data stored on iCloud is not necessarily safe or secure. As the iTC makes explicitly clear: "Apple does not guarantee or warrant that any Content you may store or access through the Service will not be subject to inadvertent damage, corruption or loss."¹²¹ iCloud also does not necessarily keep data private. According to the iTC, under certain circumstances, "Apple may access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party."¹²² Thus, employers might unwittingly surrender a considerable amount of control over their ESI by storing it on iCloud.

ESI may also be manipulated by Apple. First, Apple has the right to make changes to the actual content. The iTC provides that Apple "may pre-screen, move, refuse, **modify and/or remove** Content at any time, without prior notice and in its sole discretion, if such Content is found to be in violation of this Agreement or is otherwise objectionable."¹²³ A second provision allows Apple to take actions that, while falling short of changing the substantive content, might modify the content's metadata.¹²⁴ It states, "Apple may transmit your Content across various public networks, in various media, and **modify or change your Content** to comply with technical requirements of connecting networks or devices or computers."¹²⁵ T

Apple's reserved right to modify, change, and remove content conflicts with an employer's potential preservation duties and would likely subject it to liability for failure to preserve. An employer's duty to preserve can sometimes extend beyond actual content to include metadata.¹²⁶ In *Williams v. Sprint/United Management Co.*,¹²⁷ the United States District Court for the District of Kansas held that "when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business,¹²⁸ the producing party should produce the electronic documents with their metadata intact."¹²⁹ Failure to preserve metadata could result in sanctions as severe as default judgment.¹³⁰ Thus, the iTC contravenes an employer's duty to preserve because it allows altering of relevant documents and metadata.

In addition to the right to alter and remove content from an iCloud account, Apple may also delete a user account altogether. The iTC states, "Apple may at any time, under certain circumstances and without prior notice, immediately terminate or suspend all or a portion of your Account and/or access to the Service."¹³¹ Once an account has been terminated, the user "will lose all access to the Service and any portions thereof, including, but not limited

to, [the] Account, Apple ID, email account, and Content. In addition, after a period of time, Apple will delete information and data stored in or as a part of your account(s).”¹³²

An employer would likely be liable even if the destruction of the ESI resulted from Apple’s cancellation of the user account. In *Cyntegra, Inc. v. IDEXX Laboratories*,¹³³ the United States District Court for the Central District of California outlined a party’s responsibilities for ESI stored by a third-party vendor. In that case, the plaintiff failed to make required payments to its third-party data storage provider.¹³⁴ As a result, the vendor closed the account and deleted ESI that the plaintiff had an obligation to preserve.¹³⁵ The court found that “[b]ecause Plaintiff could have anticipated the possibility of litigation by this time, it had an affirmative duty to make payments and preserve the evidence.”¹³⁶ Having breached its duty, the plaintiff was subjected to an adverse inference sanction.¹³⁷

An employer similarly risks sanctions if it stores its ESI on iCloud. The iTC allows Apple to terminate the account, resulting in the deletion of the ESI therein.¹³⁸ And starkly similar to the situation in *Cyntegra*, the iTC specifically provides that “[i]f Apple is unable to successfully charge your credit card or payment account for fees due, Apple reserves the right to revoke or restrict access to your stored Content, delete your stored Content, or terminate your Account.”¹³⁹ With iCloud, one missed payment puts an employer at risk for significant sanctions.

2. Limitations of Liability and Consequences of Apple’s Negligence

Data loss can occur not only as a result of the type of intentional acts described above but also as a result of Apple’s negligence. While cloud vendors’ higher-level skill and attention should prevent human error, such is not always the case. For example, during the summer of 2011, a programming glitch in Dropbox’s popular cloud storage service removed password protection for all of its 25 million user accounts.¹⁴⁰ As a result, anyone could input any password for any user and have complete access to all of the stored data.¹⁴¹

If a similar mishap occurs in iCloud and ESI that is required to be preserved is destroyed, an employer would not only be held liable, but it would likely have no recourse against Apple. The iTC repeatedly limits Apple’s liability in the event of data loss. Interspersed throughout the iTC are provisions stating that the user should assume responsibility for its data and that Apple cannot be held liable:

“Apple will not be responsible to you or any third party for any damages that may result or arise out of such termination or suspension of your Account and/or access to the Service”;

“Apple shall not be responsible should such damage, corruption, loss, or removal occur” (capitalization omitted);

“It is your responsibility to maintain appropriate alternate backup of your information and data”;

“You are responsible for backing up, to your own computer or other device, any important documents, images or other Content that you store or access via the Service”;

“you, and not Apple, are solely responsible for any Content you upload, download, post, email, transmit, store or otherwise make available through your use of the Service”;

“You agree that Apple shall not be liable to you or any third party for any modification or cessation of the Service”;

“You acknowledge and agree that Apple may, without liability to you, access, use, preserve and/or disclose your Account information and Content.”¹⁴²

The iTC also contains a consolidated section titled “Limitation of Liability,” which includes the following provisions:

Some jurisdictions do not allow the exclusion or limitation of liability by service providers. To the extent such exclusions or limitations are specifically prohibited by applicable law, some of the exclusions or limitations set forth below may not apply to you.

Apple shall use reasonable skill and due care in providing the service. The following limitations do not apply in respect of loss resulting from (a) Apple's failure to use reasonable skill and due care; (b) Apple's gross negligence, wilful [sic] misconduct or fraud; or (c) death or personal injury.

You expressly understand and agree that Apple and its affiliates, subsidiaries, officers, directors, employees, agents, partners and licensors shall not be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages, including, but not limited to, damages for loss of profits, goodwill, use, data, cost of procurement of substitute goods or services, or other intangible losses (even if Apple has been advised of the possibility of such damages), resulting from: (i) the use or inability to use the service; (ii) any changes made to the service or any temporary or permanent cessation of the service or any part thereof; (iii) the unauthorized access to or alteration of your transmissions or data; (iv) the deletion of, corruption of, or failure to store and/or send or receive your transmissions or data on or through the service; (v) statements or conduct of any third party on the service; and (vi) any other matter relating to the service.¹⁴³

In addition, the iTC limits a user's ability to seek indemnification from Apple:

You agree to ... hold Apple ... harmless from any claim or demand ... made by a third party, relating to or arising from: (a) any Content you submit, post, transmit, or otherwise make available through the Service; (b) your use of the Service; (c) any violation by you of this Agreement; (d) any action taken by Apple as part of its investigation of a suspected violation of this Agreement or as a result of its finding or decision that a violation of this Agreement has occurred; or (e) your violation of any rights of another. **This means that you cannot sue Apple**, ... as a result of its decision to remove or refuse to process any information or Content, to warn you, to suspend or terminate your access to the Service, or to take any other action during the investigation of a suspected violation or as a result of Apple's conclusion that a violation of this Agreement has occurred.¹⁴⁴

As the Limitation of Liability section indicates, these exculpatory clauses may not be enforceable in every jurisdiction. An employer need not assess its enforceability everywhere, though. Rather, according to the iTC,

the relationship between you and Apple shall be governed by the laws of the State of California, excluding its conflicts of law provisions. You and Apple agree to submit to the personal and exclusive jurisdiction of the courts located within the county of Santa Clara, California, to resolve any dispute or claim arising from this Agreement.¹⁴⁵

As this provision likely anticipates, a court applies the law of the state in which it sits in order to interpret a choice-of-law provision.¹⁴⁶ Thus, to the extent that a lawsuit could be brought outside of California, notwithstanding the above provision to the contrary, that court would not apply California conflict-of-law jurisprudence. However, while specific choice-of-law standards might differ across jurisdictions, courts generally defer to the parties' choice¹⁴⁷ unless the dispute has no relation to that state or if deference would violate some public policy.¹⁴⁸ Therefore, the following analysis assumes that the choice of law provision is enforceable, and California law applies.

In California, limited liability clauses are governed by Section 1668 of the California Civil Code, which states that "[a]ll contracts which have for their object, directly or indirectly, to exempt anyone from responsibility for his own fraud, or willful injury to the person or property of another, or violation of law, whether willful or negligent, are against the policy of the law."¹⁴⁹ This prohibition has been applied unconditionally to liability disclaimers for fraud, willful injury, or violation of law,¹⁵⁰ and acts of gross negligence,¹⁵¹ "exculpatory clauses relieving a party from the consequences of his or her own *negligence* [are] unenforceable [only] when the public interest [is] involved."¹⁵² Thus, limitations of liability clauses are only enforced with respect to acts of negligence that do not implicate the public interest.

In *Tunkl v. Regents of University of California*,¹⁵³ the California Supreme Court created a framework for determining when an exculpatory clause implicates the public interest.¹⁵⁴ In that case, the plaintiff sued for injuries

resulting from the alleged negligence of hospital employees who treated him while he was a patient.¹⁵⁵ The plaintiff had signed the hospital's waiver, however, which ostensibly released it from all liability stemming from negligent or wrongful acts.¹⁵⁶ The court noted that negligence disclaimers that violate the public interest are unenforceable.¹⁵⁷ The following factors were established to determine whether such a clause implicated the public interest:

- (1) It concerns a business of a type generally thought suitable for public regulation.
- (2) The party seeking exculpation is engaged in performing a service of great importance to the public, which is often a matter of practical necessity for some members of the public.
- (3) The party holds himself out as willing to perform this service for any member of the public who seeks it, or at least any member coming within certain established standards.
- (4) As a result of the essential nature of the service, in the economic setting of the transaction, the party invoking exculpation possesses a decisive advantage of bargaining strength against any member of the public who seeks his services.
- (5) In exercising a superior bargaining power the party confronts the public with a standardized adhesion contract of exculpation, and makes no provision whereby a purchaser may pay additional fees and obtain protection against negligence.
- (6) Finally, as a result of the transaction, the person or property of the purchaser is placed under the control of the seller, subject to the risk of carelessness by the seller or his agents.¹⁵⁸

Finding that all factors favored the plaintiff, the court held that the waiver violated the public interest and was therefore unenforceable.¹⁵⁹

Here, the iTC's limitation of liability section provides greater user protection than the California statute and associated case law. While the law only prohibits disclaimers of liability for negligence where the public interest is implicated, the Limitations of Liability provision does not release Apple from negligence liability under any circumstance.¹⁶⁰ On its own, this clause is particularly noteworthy. If this were the only section relating to Apple's liability for data loss, iCloud would be a consumer's magic bullet. However, as indicated above, the iTC contains similar disclaimers throughout the contract that are not qualified by any finding of Apple's level of culpability, along with a section limiting indemnification under certain circumstances. Under California law, exculpatory provisions unqualified by any level of culpability are presumed to release liability for negligence as long as "the act of negligence [is] reasonably related to the object or purpose for which the release is given."¹⁶¹ The iTC repeatedly makes clear that one of its major objects or purposes is to absolve Apple of any responsibility for loss or destruction of ESI. Therefore, the provisions would likely extend to loss or destruction, where such loss or destruction was the result of negligence. Therefore, to determine whether Apple may disclaim its own negligence under California law, it is necessary to consider whether the storage and potential loss of data on iCloud implicates the public interest.

The *Tunkl* factors, when applied to Apple and iCloud, demonstrate that the public interest likely is not implicated. The clear absence of public regulation and importance to the public, as described in the first two factors, suggest a lack of public interest.¹⁶² The third factor regarding availability for any member of the public, however, is clearly satisfied.¹⁶³ The fourth factor, although associated with unbalanced bargaining power (which might exist depending on the user), is premised on the essential nature of the service. iCloud cannot reasonably be deemed an essential service, given that local storage of ESI has been and will likely continue to be easy, cheap, prevalent, and practicable. Thus, "it 'is not a compelled, essential service' but 'a voluntary relationship between the parties.'"¹⁶⁴ As to the fifth factor, regarding contracts of adhesion,¹⁶⁵ it remains to be seen whether Apple will provide users the option of paying additional fees to obtain protection against negligence.¹⁶⁶ However, as a practical matter, likely only large employers will have sufficient leverage to obtain, and provide Apple with sufficient incentive to offer, such an option.¹⁶⁷ As such, this factor may demonstrate that the public interest is implicated, but likely only for small- and medium-sized businesses.

While the final factor, regarding the seller's control over the purchaser's property, might appear apt with iCloud, case law involving items lost while located in paid storage indicates otherwise. In *Guivi v. Spectrum Club*

Holding Co.,¹⁶⁸ the California Court of Appeals applied the *Tunkl* factors where a health club member's belongings were allegedly stolen from her paid rental locker.¹⁶⁹ In considering the final factor, the court distinguished the health club from other sellers such as hospitals, day care facilities, and automobile repair shops, which were deemed to possess the requisite control over the purchaser's property.¹⁷⁰ In those instances, the purchaser "[cedes] control to the [seller]," "is powerless to control the extent to which the [seller] does or does not act negligently;" and "is in no position to control the extent to which its protection from theft or damage is negligently performed."¹⁷¹ However, the plaintiff in *Guivi* was not limited in her choice of health clubs, could have left her belongings in another location under her exclusive control, and merely ceded control to the health club for her own convenience.¹⁷² As such, the court held that the sixth factor was not satisfied and that the *Tunkl* factors generally did not indicate that the public interest was implicated.¹⁷³

Similarly, in *Magliocco v. American Locker Co., Inc.*,¹⁷⁴ the plaintiffs' money was taken from a paid locker at a bus station when an employee opened the locker for an individual misrepresenting himself as the renter.¹⁷⁵ The court found that, because the plaintiffs "never placed their money under the control of [the defendant and] retained the key to the locker, never relinquishing primary physical control over its contents," the sixth factor was not satisfied.¹⁷⁶

Storing ESI on iCloud is not dissimilar to storing belongings in the rented lockers in the above cases. Just like the court found in *Guivi*, employers may choose to store their ESI with many remote storage vendors, may opt to retain control over their ESI by storing it on local servers or hard drives, and would be contracting with Apple merely out of convenience. Similar to the reasoning in *Magliocco*, employers possess the username and password to their iCloud account, thereby retaining primary control over accessing, updating, adding, or removing content therein. Therefore, the sixth factor likely would not be deemed satisfied.

With only the third and, possibly in some instances, the fifth factor satisfied, the courts are more likely to find that ESI storage on iCloud does not implicate the public interest. Therefore, Apple likely may disclaim its liability resulting from its own negligence. As such, an employer would not be entitled to either direct relief for its own injuries resulting from the loss of ESI or indemnification for e-discovery sanctions imposed by a third party. iCloud therefore fails to adequately diminish liability exposure, as ideally expected from a cloud computing product.

III. RECOMMENDATIONS

A. Recommendation 1: Negotiate Better Terms with Apple

As discussed in Part II-A, employers increasingly have been recognizing the advantages of using Apple products. As evidenced by the iTC, however, using iCloud poses considerable e-discovery risks.¹⁷⁷ Thus, in the interest of continuing to take advantage of the broader benefits Apple offers, employers may seek to mitigate their iCloud-related e-discovery risks by negotiating the terms of the iTC. While cloud computing providers are widely known for their contractual inflexibility,¹⁷⁸ negotiation is strongly advised¹⁷⁹ and often possible.¹⁸⁰ The possibility and nature of negotiation ultimately will depend on a variety of factors, of which two of the most salient are (1) the size of the employer¹⁸¹ and (2) whether the employer is a public or private entity. As demonstrated in the case study below, larger and public entities might have greater bargaining strength at the negotiating table than smaller and private ones.

1. A Tale of Two Cities: Size Does Matter

Over the past few years, Google has offered employers a cloud computing service called Google Apps.¹⁸² Its Terms of Service contain a variant of the type of general disclaimer commonly found in standardized service agreements, stating:

12. Indemnification.

12.1 By Customer. Customer will indemnify, defend, and hold harmless Google from and against all liabilities, damages, and costs (including settlement costs and reasonable attorneys' fees) arising out of a third party claim . . . regarding Customer Data . . .

13.1 Limitation on Indirect Liability. Neither party will be liable under this agreement for lost revenues or indirect, special, incidental, consequential, exemplary, or punitive damages, even if the party knew or should have known that such damages were possible and even if direct damages do not satisfy a remedy.

13.2 Limitation on Amount of Liability. Neither party may be held liable under this agreement for more than the amount paid by customer to Google hereunder during the twelve months prior to the event giving rise to liability.¹⁸³

Google Apps has been adopted by over 5 million “businesses”¹⁸⁴ (a term seemingly meant to include governmental bodies),¹⁸⁵ the vast majority of whom likely merely accepted Google’s preset terms.¹⁸⁶ However, at least two entities are known to have engaged in negotiations: the City of Los Angeles¹⁸⁷ and the City of Pittsburgh.¹⁸⁸ The two resulting contracts, as discussed below, illustrate the disparate levels of success at reducing client-side risk.

i. The City of Los Angeles Contract (“LA Contract”)¹⁸⁹

In November 2009, the City of Los Angeles entered into a contract with Google and Google’s contractor Computer Science Corporation (“CSC”) to provide cloud computing services for its 30,000 employees for five years at a cost of \$7,250,000.¹⁹⁰ The contract is divided into one main part and several appendices. Those sections relevant to this discussion include the main agreement with CSC (“CSC Agreement”), Appendix B – Statement of Work (“Statement of Work”),¹⁹¹ and Appendix J – Google Services Agreement (“Google Agreement”).¹⁹²

The Statement of Work indicates that the City of Los Angeles wished to integrate e-discovery risk-reducing design features into the services they were to receive. It opted for both the e-Discovery Solution – which enables the City to search ESI based on content, sender and/or recipient, date range, and metadata; store search results with any metadata; and add and delete from search results to create an e-Discovery set – and the Archive and Backup Solution – which enables the City to store and retrieve e-mail data; archive data based on certain data characteristics; retrieve or e-discover archived data; view and manipulate archived data; and restore archived data.¹⁹³ By integrating these solutions into the cloud computing product, the City can preemptively reduce e-discovery risk by diminishing the likelihood of data loss through more-effective ESI storage and organization. The City is thereby more likely to avoid the considerable legal costs associated with litigating collateral e-discovery issues.

The negotiated terms in the CSC Agreement also reduce risk, not by diminishing the likelihood of data loss, but by reducing the exposure to liability in the event of data loss. Much of the CSC Agreement resembles the terms of Google’s standard contract. For example, the limitation of indirect liability provision has been modified merely to specify some of the bases for liability that are disclaimed:

Neither party shall be liable hereunder for penalties or for special, indirect, consequential or incidental losses or damages **including, but not limited to, lost profits, lost or damaged data, failure to achieve cost savings, loss of use of facility or equipment, or the failure or increased expense of operations, regardless of whether any such losses or damages are characterized as arising from strict liability or otherwise**, even if a party is advised of the possibility of such losses or damages, or if such losses or damages are foreseeable.¹⁹⁴

However, other provisions have significantly changed the balance of risk, notably in the City’s favor. As opposed to the \$1000 liability cap provided by the standard contract, the CSC Agreement caps liability at \$7.7 million.¹⁹⁵ Moreover, whereas Google’s standard contract provides that the user will indemnify and hold Google harmless for all damages, liabilities, and costs, the CSC Agreement provides that CSC will indemnify the City “from . . . all third party suits and causes of action, claims, losses, demands and expenses, including but not limited to, attorney’s fees and cost of litigation, damage or liability of any nature whatsoever, for lost City Data” up to \$7.7 million.¹⁹⁶

The Google Agreement contains provisions similar to both its standard contract as well as to the CSC Agreement. As opposed to the CSC Agreement, the Google Agreement does contain the standard contract's indemnification clause, which provides that the City will hold Google harmless from all liabilities relating to the City's data.¹⁹⁷ It also contains the same indemnification provision found in the CSC Agreement, however, and states that Google will indemnify the City for liability resulting from lost data.¹⁹⁸ Furthermore, the Google Agreement's limitation of indirect liability section also uses the same language as its standard contract, providing that "[n]either party will be liable under this agreement for lost revenues or indirect, special, incidental, consequential, exemplary, or punitive damages, even if the party knew or should have known that such damages were possible and even if direct damages do not satisfy a remedy."¹⁹⁹ The agreement also increases Google's liability cap, however, to "[t]he amount paid by customer to reseller during the twelve months prior to the event giving rise to liability."²⁰⁰

Both the CSC Agreement and the Google Agreement contain unfavorable provisions, mostly borrowed from Google's standard contract, as well as favorable ones. While reconciling these clauses with one another might prove challenging,²⁰¹ Los Angeles' ability to advance its risk-based interests at all is noteworthy given the difficulty of negotiating with cloud computing providers. Unfortunately, this level of success might not always be so easily replicated, especially with smaller clients, as demonstrated by the following case study.

ii. The City of Pittsburgh Contract ("Pittsburgh Contract")²⁰²

In August 2011, the City of Pittsburgh entered into a contract with Google – and its contractor Daston Corporation ("Daston") – to provide cloud computing services for its 3,000 employees²⁰³ for 3.25 years at a cost of \$806,800.²⁰⁴ The Pittsburgh Contract is split into several parts including "Exhibit A: Scope of Work" ("Exhibit A") and an addendum ("Addendum"), the latter closely resembling the Google standard contract.

Exhibit A largely outlines the structure and design features of the cloud computing product, just as the Statement of Work did in the LA Contract.²⁰⁵ The City's representatives also must have anticipated the e-discovery implications of storing ESI in the cloud²⁰⁶ as they too opted for the e-Discovery and Archive and Backup Solutions.²⁰⁷ However, notwithstanding these beneficial design features, the contract's Addendum fails to dispel many of the legal risks as did the LA Contract. It contains the same limitation of indirect liability as Google's standard contract²⁰⁸ and the same intermediate liability cap as the LA Contract's Google Agreement.²⁰⁹ The indemnification section does provide that Google will indemnify the City, but only for intellectual property-related liability as opposed to data loss-related liability.²¹⁰

The LA Contract clearly provides better legal protections than the Pittsburgh Contract. While there might be multiple explanations for why Los Angeles had greater success than Pittsburgh, it is reasonable to infer that the cities' respective sizes played a role. The Los Angeles cloud computing product cost nearly ten times more and served ten times more employees than the Pittsburgh product.²¹¹ The City of Los Angeles likely leveraged its large bid to increase its bargaining power, which resulted in several favorable indemnity and liability provisions. The City of Pittsburgh, however, did not come out completely empty-handed. The risk-reducing design features might be all that it truly needs in order to avoid extra litigation costs and potential sanctions. Thus, while large employers might be more likely to procure favorable legal provisions, smaller employers are by no means precluded from creating a desirable arrangement through other methods.

2. Differences Between Private and Public Employers

Cloud computing contract negotiation might be one of the few examples where being subject to heightened regulation offers logistical advantages. In 2002, Congress passed the Federal Information Security Management Act ("FISMA")²¹² in order to "provide for development and maintenance of minimum controls required to protect Federal information and information systems."²¹³ Under FISMA, the Director of the Office of Management and Budget is authorized, in collaboration with the National Institute of Standards and Technology ("NIST"), to "develop[] and oversee[] the implementation of policies, principles, standards, and guidelines on information security."²¹⁴ All federal agencies are required to integrate information security protections for their information and information systems in accordance with those promulgated rules.²¹⁵ NIST has promulgated a considerable amount of information security guidance,²¹⁶ and is in the process of developing a set of standards specifically for cloud

computing systems.²¹⁷ While the breadth and technical nature of the relevant guidelines sets them outside the scope of this article, it is reasonable to infer that increases in information security reduce e-discovery risks.

A cloud computing service provider must offer a FISMA-compliant product in order to contract with a federal agency. Google,²¹⁸ Microsoft,²¹⁹ and, recently, Amazon²²⁰ all offer FISMA-compliant cloud computing products. However, these providers do not need to make all of their cloud computing products FISMA-compliant (only those offered to federal agencies), just as not all entities are required to use FISMA-compliant products (only federal agencies). Therefore, providers are apt to design multiple products, both FISMA-compliant and not. Federal agencies therefore have an automatic advantage over other entities when negotiating a cloud computing contract.

State and local governments may also take advantage of the FISMA regulations. While these public entities are not required to comply with FISMA, cloud computing providers have been receptive to offering them FISMA-compliant products. For example, under its contract with the City of Pittsburgh, Google is required to provide a FISMA-compliant product, and any failure in maintaining compliance entitles the City to terminate the agreement.²²¹

Cloud computing providers are not as likely to offer FISMA-compliant products to private entities. As an initial matter, the standard contracts are unlikely to be FISMA-compliant. For example, Google's standard contract merely provides that it "will adhere to reasonable security standards ... [with] at least industry standard systems" and do no more than "comply with all laws and regulations applicable to its provision, or use, of the Services, as applicable."²²² Beyond that, private employers wishing to negotiate for a provider's FISMA-compliant product might have an uphill battle ahead of them.

* * *

Because Apple has only recently emerged as a serious player in the cloud computing market,²²³ it remains to be seen whether and to what degree it will be amenable to negotiating its iCloud contract. The preceding case studies and analyses illuminate some broader market trends, however, and suggest the type of negotiating environment that an employer can expect with Apple. For example, while large employers might be able to use their leverage to reduce liability risk, employers both large and small might have the option of an iCloud version with built-in risk-reducing design features. Further, public employers, and in particular federal agencies, might hold the best seat, assuming Apple is able to offer a FISMA-compliant version of iCloud.

B. Recommendation 2: Alternatives to iCloud

Notwithstanding the previous section's analysis, negotiated cloud computing contracts are relatively uncommon²²⁴ and employers need to be willing to make their purchasing determinations based on the product's standard terms. As such, employers have three options: (1) use iCloud under the standard terms found in the iTC, (2) use a different cloud computing provider subject to its standard terms, or (3) decline to use cloud computing altogether.

While Apple might be well positioned to offer businesses a cloud computing product,²²⁵ employers should not be too quick to jump onto the Apple bandwagon. As discussed above, iCloud's technological limitations and contractual disclaimers might leave employers at risk.²²⁶ iCloud might even pose additional e-discovery risks related to security, data sovereignty, cloud sprawl, and privacy.²²⁷ Moreover, because of Apple's inexperience with providing a successful cloud computing product, it lacks the type of infrastructure possessed by some of its more seasoned competitors.²²⁸ To make matters worse, Apple is also notorious for scorning businesses in favor of consumer clients.²²⁹

While Apple might not be the right choice for many businesses, the alternatives might not be much better. Limitation of liability provisions are ubiquitous among cloud computing contracts, including those used by Google.²³⁰ Employers cannot evade these clauses even if they choose to contract with providers that are more enterprise-oriented,²³¹ as opposed to consumer-focused providers like Apple. In fact, beneath the surface the differences might be meaningless. For example, iCloud data is not actually stored on servers owned by Apple, but

rather on those of its competitors Microsoft and Amazon.²³² With providers' equipment and contractual terms seemingly interchangeable, employers might not have all that many options.

With all these uncertainties and complexities, some employers might understandably opt to forgo cloud computing altogether. After all, cloud computing might raise additional concerns not discussed in this article, depending on an employer's particular circumstances.²³³ It might be prudent simply to wait for cloud computing providers to provide better legal protections for their clients, as some observers anticipate.²³⁴

CONCLUSION

In theory, cloud computing reduces the risk of ESI destruction and spoliation liability for employers in the event of data loss. Unfortunately, neither iCloud nor competing products fully offer those protections. Instead, under the iTunes, Apple reserves the right to modify and delete user data without liability, even in the event of its own negligence. Other providers have included similar provisions shielding them from liability. Businesses will likely find similar unfavorable terms and negotiation positions no matter which service provider they choose.

So is cloud computing just a whole lot of hype – a catchy term and clever marketing to hide the legal risks? Is cloud computing problematic, or are the identified risks inherent not to the technology but to ourselves? After all, computers do not delete data – people do. Evolving technologies, promising more security and less risk, might very well be perpetuating our own willful blindness. Optimal risk reduction will not come from buying the newest gadget but rather from implementing training programs and instilling a corporate culture that promotes diligent handling of data and proper oversight. These types of initiatives should receive further academic research and corporate consideration. Cloud computing might offer certain advantages and disadvantages. However, employers that are mindful not only of technological limitations, but of employee behavior, can realize cloud computing's full potential.

* Daniel Carmeli is an associate at Fulbright & Jaworski L.L.P. He thanks Rhonda Wasserman, Professor of Law at the University of Pittsburgh School of Law, for her invaluable instruction and guidance. He thanks the Boston College Intellectual Property and Technology Forum staff for their hard work in editing this article. He would also like to thank his family for all their love and support.

¹ *Pittsburgh, C. & St. L.R. Co. v. Barrett & Walton*, 36 Ohio St. 448 (1881).

² Frederick Schauer & Virginia J. Wise, *Legal Positivism as Legal Information*, 82 CORNELL L. REV. 1080, 1107 (1997) ("Even without the Internet, which increases by several orders of magnitude the phenomenon we identify, the computer has dramatically increased the availability and ease of accessibility of nonlegal materials."); Jack B. Weinstein, *Some Benefits and Risks of Privatization of Justice Through ADR*, 11 OHIO ST. J. ON DISP. RESOL. 241, 273 (1996) ("Computers can also help increase the courts' accessibility to non-English speaking litigants and defendants.").

³ Jonathan A. Franklin, *One Piece of the Collection Development Puzzle: Issues in Drafting Format Selection Guidelines*, 86 LAW LIBR. J. 753, 760 (1994) ("The benefits of CD-ROMs are their flat cost, ruggedness, and accessibility to multiple concurrent users, if networked.").

⁴ See, e.g., Debra Moss Curtis & Judith R. Karp, *In a Case, on the Screen, Do They Remember What They've Seen? Critical Electronic Reading in the Law Classroom*, 30 HAMLINE L. REV. 247, 275 (2007) ("The availability of CD-ROMs, external disc drives and flash drives that can easily transfer electronic text to an always-accessible format makes memorializing, categorizing and transporting electronic text a reality.").

⁵ Jeff W. LeBlanc, *The Pursuit of Virtual Life, Liberty, and Happiness and Its Economic and Legal Recognition in the Real World*, 9 FLA. COASTAL L. REV. 255, 258 (2008) ("The rapid growth of the Internet in the 1990s resulted in an increase in business and social activities that took advantage of the Internet's omnipresent ease of use and accessibility."); *Reconciliation on-Line: Reflections and Possibilities*, 28 INT'L J. LEGAL INFO. 213, 224 (2000) ("In an obvious sense, the mere connection of remote communities to the Internet increases accessibility.").

⁶ See, e.g., Press Release, Mimecast, Young Employees' 'Social' Approach to Email Puts UK Business at Risk (Feb. 23, 2011), <http://www.mimecast.com/News-and-views/Press-releases/Dates/2011/2/-Young-employees-social-approach-to-email-puts-UK-business-at-risk> (finding that "79 per cent of people send work emails from their personal email accounts, with 1 in 5 saying they do this on a regular basis").

⁷ See, e.g., PONEMON INSTITUTE, *THE STATE OF USB DRIVE SECURITY: U.S. SURVEY OF IT AND IT SECURITY*

PRACTITIONERS 3 (2011), available at http://media.kingston.com/images/usb/pdf/MKP_272_Ponemon_WP.pdf (38% of surveyed companies provide employees with an approved USB drive for use in the workplace).

⁸ Press Release, The Masters Conference, Masters Conference Announces Huron Legal as a Sponsor at 2011 Event (June 21, 2011), available at <http://www.themastersconference.com/press-releases/377-masters-conference-announces-huron-legal-as-a-sponsor-at-2011-event> (“The convergence of cloud computing and mobile computing have provided great improvements in accessibility while lowering the total cost of ownership for computer systems and services.”).

⁹ As the National Institute of Standards and Technology (“NIST”) definition indicates, cloud computing models vary based on the type of resources they provide. For purposes of this article, cloud computing models that only provide storage will be referred to as “cloud storage” while those that offer additional applications and services will be referred to with the broader term of “cloud computing.”

¹⁰ PETER MELL & TIMOTHY GRANCE, NIST, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), available at <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

¹¹ See, e.g., Nerino J. Petro, Jr., *Using Online Storage to Make Your Mobile Life Easier*, LAW PRAC., March/April 2010, at 19, available at http://www.americanbar.org/publications/law_practice_home/law_practice_archive/lpm_magazine_articles_v36_is2_pg19.html (listing nine popular online storage service providers); Press Release, Dropbox, Dropbox Reveals Tremendous Growth With Over 200 Million Files Saved Daily by More Than 25 Million People: Service Spans 175 Countries and Launches in Spanish, German, French and Japanese (Apr. 18, 2011), available at <http://www.dropbox.com/news/20110418> (Dropbox, a popular online storage service provider claims to have 25 million users in 175 countries).

¹² See Press Release, Amazon.com Inc., Introducing Amazon Cloud Drive, Amazon Cloud Player for Web, and Amazon Cloud Player for Android (Mar. 29, 2011), available at <http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1543596&highlight=>; Claire Cain Miller, *Amazon Introduces a Digital Music Locker*, N.Y. TIMES, Mar. 29, 2011, <http://bits.blogs.nytimes.com/2011/03/29/amazon-introduces-a-digital-music-locker>.

¹³ Ben Sisario, *Google’s Digital Music Service Falls Short of Ambition*, N.Y. TIMES, May 11 2011, at B8. Note that this service has since been rebranded as “Google Play” and offers storage of files other than music.

¹⁴ About Music Beta by Google, <http://music.google.com/about> (last visited Dec. 8, 2011).

¹⁵ Google Docs is Google’s collection of cloud-based document editing software that is now accessible through the cloud storage service Google Drive. Docs Blog, Upload and Store your Files in the Cloud with Google Docs (Jan. 12, 2010), <http://googledocs.blogspot.com/2010/01/upload-and-store-your-files-in-cloud.html>; see also An Overview of Google Docs – Google Docs Help, <http://support.google.com/docs/bin/answer.py?hl=en&answer=49008> (last visited Dec. 8, 2011); Google Docs is also part of a larger cloud computing product offered to businesses called Google Apps. See *infra* note 180.

¹⁶ Press Release, Apple, Inc., iPhone 4S First Weekend Sales Top Four Million (Oct. 17, 2011), available at <http://www.apple.com/pr/library/2011/10/17iPhone-4S-First-Weekend-Sales-Top-Four-Million.html>.

¹⁷ See, e.g., David Sarno, *Los Angeles Adopts Google E-mail System for 30,000 City Employees*, L.A. TIMES, Oct. 27, 2009, <http://latimesblogs.latimes.com/technology/2009/10/city-council-votes-to-adopt-google-email-system-for-30000-city-employees.html> (City of Los Angeles, with 30,000 employees, has recently contracted for delivery of a Google Apps cloud solution); NASA Flagship Initiatives, <http://www.nasa.gov/open/plan/nebula.html> (last visited Dec. 8, 2011) (NASA has launched its own cloud computing platform); Vivek Kundra, The White House, Moving to the Cloud (May 13, 2010), <http://www.whitehouse.gov/blog/2010/05/13/moving-cloud> (describing efforts for entire federal government to use cloud computing).

¹⁸ KPMG, CLARITY IN THE CLOUD: THE IMPACT, OPPORTUNITY AND RISK OF CLOUD 3 (2011), <http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/oracle-openworld/Documents/clarity-in-the-cloud.pdf> (a recent survey conducted by KPMG found that “81% of businesses are either planning their initial forays, are in early or advanced stages of experimentation or have full implementations.”).

¹⁹ See, e.g., David Narkiewicz, *Fearless Technology Predictions for 2014*, PA. LAW., November/December 2010, at 18, 21, available at <http://e-conditionsbyfry.com/Olive/ODE/PAB/default.aspx?href=PAB%2F2010%2F11%2F01&pageno=20&entity=Ar02000&view=entity> (“Small firms and solos may use cloud computing primarily as a backup service, but large firms and medium-sized firms, particularly those with multiple offices, will keep virtually all of their client files and firm

information in cloud computing for easy accessibility among the offices and for lawyers who are on the road or in court.”).

²⁰ See, e.g., Dwayne D. Stresman & William C. Lentine, *A Primer on IT Outsourcing: What to Look for Before You Leap*, MICH. B.J., July 2011, at 38, 39, available at <http://www.michbar.org/journal/pdf/pdf4article1874.pdf> (“Essentially, cloud computing has brought ITO [information technology outsourcing] accessibility down to the medium- and even small-business level because of its relatively inexpensive nature.”); Andrew C. DeVore, *Cloud Computing: Privacy Storm on the Horizon?*, 20 Alb. L.J. Sci. & Tech. 365, 367 (2010) (“Cloud computing also offers potentially significant advantages with regard to cost savings and efficiency”); IBM, THE BENEFITS OF CLOUD COMPUTING: A NEW ERA OF RESPONSIVENESS, EFFECTIVENESS, AND EFFICIENCY IN IT SERVICE DELIVERY 10 (2009), available at <ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/diw03004usen/DIW03004USEN.PDF> (“Studies have documented that cloud computing can save 80 percent on floor space and 60 percent on power, while tripling asset utilization.”).

²¹ Mark Veverka, Barron’s, *A Private Party* (Oct. 25, 2010), http://online.barrons.com/article/SB50001424053111904502004575562243330821352.html#articleTabs_panel_article%3D1 (listing Revlon and Charles Schwab as examples of U.S. companies that have adopted cloud computing).

²² SYMANTEC, STATE OF CLOUD SURVEY 8 (2011), available at http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=stateofcloud2011&om_ext_cid=biz_soc_med_twitter_facebook_marketwire_linkedin_2011Sep_worldwide_stateofcloudsurvey.

²³ Brad Stone & Ashlee Vance, *Companies Slowly Join Cloud-Computing*, N.Y. TIMES, Apr. 19, 2010, at B1.

²⁴ See *supra* note 10. For the purposes of this article, this pure form of cloud computing is presumed.

²⁵ The ensuing analysis assumes that an employer will not be negligent in its selection of its cloud computing provider. See RESTATEMENT (SECOND) OF TORTS § 411 (Negligence in Selection of Contractor).

²⁶ See, e.g., *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 522 (D. Md. 2010).

²⁷ A PROJECT OF THE SEDONA CONFERENCE WORKING GROUP ON ELEC. DOCUMENT RETENTION & PROD., THE SEDONA PRINCIPLES: SECOND EDITION, BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION 14 cmt. 1.c (2007), available at <https://thesedonaconference.org/download-pub/81> [hereinafter *Sedona Principles*].

²⁸ See, e.g., *Krumwiede v. Brighton Associates, L.L.C.*, 05 C 3003, 2006 WL 1308629, at *9 (N.D. Ill. May 8, 2006).

²⁹ Sometimes, even an employer’s lawyers cannot be fully trusted to safeguard the devices storing ESI. See, e.g., *Tricia Bishop, Law Firm Loses Hard Drive with Patient Records: Attorneys represent St. Joseph cardiologist sued for malpractice*, BALTIMORE SUN, Oct. 10, 2011, available at <http://www.baltimoresun.com/news/maryland/bs-md-stent-hard-drive-20111010,0,599052.story> (lawyer left a portable hard drive containing “medical records related to the stent malpractice claims, along with patient names, addresses, dates of birth, social security numbers and insurance information.”).

³⁰ Human error has recently been found to be the leading cause of data loss, accountable for 40% of all loss. See Press Release, Kroll Ontrack, Technology Users Believe Human Error Is The Leading Cause Of Data Loss (July 20, 2010), <http://www.krollontrack.com/company/news-releases/?getpressrelease=61462>.

³¹ *Yu Chen v. LW Rest., Inc.*, 10 CV 200 ARR, 2011 WL 3420433, at *6, *10, *12, *20–21 (E.D.N.Y. Aug. 3, 2011) (finding that the loss was at least grossly negligent; therefore, the court precluded the employer from proffering related evidence, granted an adverse inference, and awarded attorney’s fees); see also Press Release, Kingston Technology, Nearly Half of Organizations Have Lost Sensitive or Confidential Information on USB Drives in Just the Past Two Years (Aug. 9, 2011), <http://www.kingston.com/us/company/press/article/2661> (recent survey finding that “[n]early 50 percent of organizations confirmed lost drives containing sensitive or confidential information in the past 24 months.”).

³² *Wilson v. Thorn Energy, LLC*, 08 CIV 9009 (FM), 2010 WL 1712236, at *2–4 (S.D.N.Y. Mar. 15, 2010) (finding that the destruction of evidence resulting from the flash drive’s failure amounted to gross negligence or willfulness and, thereby, precluding the employer from proffering related evidence).

³³ *Harkabi v. SanDisk Corp.*, 08 CIV. 8203 WHP, 2010 WL 3377338, at *5, *7 (S.D.N.Y. Aug. 23, 2010) (finding that the employer was at least negligent and, thereby, granted the plaintiffs’ motion for an adverse inference).

³⁴ *Bryant v. Gardner*, 587 F. Supp. 2d 951, 968–69 (N.D. Ill. 2008) (although destruction did not amount to willfulness or bad faith, court still precluded defendants’ use of evidence on the topic and awarded plaintiff attorney’s fees).

³⁵ See, e.g., GFI SOFTWARE, THE THREAT POSED BY PORTABLE STORAGE DEVICES 3–4 (2009), available at <http://www.gfi.com/whitepapers/threat-posed-by-portable-storage-devices.pdf>.

³⁶ See, e.g., Frank Brick, Information Systems Security, Distributed Data: The New Security Frontier, <http://www.infosectoday.com/Articles/DistributedData.htm> (last visited Dec. 8, 2011) (“Internal IT staff has many responsibilities” now that “business-critical information is forever on the move from mainframes to departmental servers, from notebook computers to on-site and off-site backup and vaulting systems.”).

³⁷ ROLF HARMS & MICHAEL YAMARTINO, MICROSOFT, THE ECONOMICS OF THE CLOUD 7 (2010), available at <http://www.microsoft.com/presspass/presskits/cloud/docs/The-Economics-of-the-Cloud.pdf> (discussing how resource-pooling makes cloud computing cheaper).

³⁸ See, e.g., Barry Richard, Janet Kelley & Clyde Lea, *Privileged and Confidential Information*, in 2 Successful Partnering Between Inside and Outside Counsel § 28:41 (Robert L. Haig, ed. 2011) (“It is common practice in some companies and law firms for employees to take computer files home or travel on disks, flash drives or notebook computers”).

³⁹ See *supra* note 9.

⁴⁰ See *supra* note 5.

⁴¹ As discussed above, employers have been liable for sanctions as a result of the loss of just one device. See *supra* notes 31–34. It is also worth noting that loss of data can have practical costs as well. See, e.g., David M. Smith, *The Cost of Lost Data: The Importance of Investing in that “Ounce of Prevention,”* 6 GRAZIADIO BUS. REV. (2003), <http://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data> (“Added together, the costs due to technical services, lost productivity, and the value of lost data [for one data loss incident] bring the expected cost for each data loss incident to \$3,957”).

⁴² Of course there is the inevitable actual cost of replacing the device itself.

⁴³ FED. R. CIV. P. 26(g)(1).

⁴⁴ FED. R. CIV. P. 26 advisory committee note (1983).

⁴⁵ *Id.*; see also *Hewlett Packard Co. v. Factory Mut. Ins. Co.*, 04 CIV. 2791 TPG/DF, 2006 WL 1788946, at *14 (S.D.N.Y. June 28, 2006); *St. Paul Reinsurance Co., Ltd. v. Commercial Fin. Corp.*, 198 F.R.D. 508, 516 (N.D. Iowa 2000); *Poole ex rel. Elliott v. Textron, Inc.*, 192 F.R.D. 494, 503 n.11 (D. Md. 2000); *Dixon v. Certainteed Corp.*, 164 F.R.D. 685, 691 (D. Kan. 1996).

⁴⁶ Patrick Oot et. al., *Mandating Reasonableness in A Reasonable Inquiry*, 87 DENV. U. L. REV. 533, 539 (2010).

⁴⁷ Jonathan M. Redgrave, *The Sedona Conference Working Group on Electronic Document Retention and Production*, 4 SEDONA CONF. J. 197, 223 (2003); see also Molly E. Crane, *Let's Be Reasonable About It: Defining the Reasonable Inquiry in an Age of Disaggregation*, 23 GEO. J. LEGAL ETHICS 555, 561 (2010) (“Companies may have key information not only in their primary electronic storage servers, but also on personal and company-issued laptops, e-mail systems, external hard drives, and other information systems.”).

⁴⁸ Kenneth J. Withers, *Computer-Based Discovery in Federal Civil Litigation*, 2000 FED. CTS. L. REV. 2, *II.B.1 (2000).

⁴⁹ See, e.g., *AAB Joint Venture v. United States*, 75 Fed. Cl. 432, 443 (2007) (citing *Linnen v. A.H. Robins Co., Inc.*, 97-2307, 1999 WL 462015, at *6 (Mass. Super. June 16, 1999)) (“To permit a party ‘to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results.’”).

⁵⁰ See e.g., *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 107 (2d Cir. 2002) (citation omitted) (courts will generally look to whether: “(1) [] the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) [] the records were destroyed ‘with a culpable state of mind’; and (3) [] the destroyed evidence was ‘relevant’ to the party’s claim or defense such that a reasonable trier of fact could find that it would support that claim or defense”).

⁵¹ See, e.g., *id.* at 108 (citation omitted); *Leon v. IDX Sys. Corp.*, 464 F.3d 951, 958 (9th Cir. 2006); *Chrysler Realty Co., LLC v. Design Forum Architects, Inc.*, 06-CV-11785, 2009 WL 5217992, at *3 (E.D. Mich. Dec. 31, 2009); *Brown v. Chertoff*, 563 F. Supp. 2d 1372, 1381 (S.D. Ga. 2008); *CentiMark Corp. v. Pegnato & Pegnato Roof Mgmt.*, No. 05 Civ. 708, 2008 WL 1995305, at *10 (W.D. Pa. May 6, 2008); *Mazloun v. D.C. Metro. Police Dep’t*, 530 F. Supp. 2d 282, 293 (D.D.C. 2008); *E.E.O.C. v. LA Weight Loss*, 509 F. Supp. 2d 527, 538–39 (D. Md. 2007); *Teague v. Target Corp.*, No. 06 Civ. 191, 2007 WL 1041191, at *2 (W.D.N.C. Apr. 4, 2007); *Samsung Elec. Co. v. Rambus Inc.*, 439 F. Supp. 2d 524, 540 (E.D. Va. 2006). Note, however, that some courts require higher levels of culpability demonstrated by bad faith or gross negligence. See, e.g., *Condrey v. Suntrust Bank of Georgia*, 431 F.3d 191, 203 (5th Cir. 2005); *Aramburu v. Boeing Co.*, 112 F.3d 1398, 1407 (10th Cir. 1997); *United States v. Esposito*, 771 F.2d 283, 286 (7th Cir. 1985); *Bryant v. Nicholson*, No. 07 Civ. 0183, 2008 WL 465270, at *5 (N.D. Tex. Feb. 21, 2008); *Chan v. Triple 8 Palace, Inc.*, 03CIV6048(GEL)(JCF), 2005 WL 1925579, at *8 (S.D.N.Y. Aug. 11, 2005).

⁵² Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., 685 F. Supp. 2d 456, 464 (S.D.N.Y. 2010).

⁵³ Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (citation omitted); FED.R.CIV.P. 34(a)(1); see also FED.R.CIV.P. 26(a)(1)(A)(ii).

⁵⁴ Compare Prokosch v. Catalina Lighting, Inc., 193 F.R.D. 633, 636 (D. Minn. 2000) (“under Rule 34, ‘control’ does not require that the party have legal ownership or actual physical possession of the documents at issue; rather, documents are considered to be under a party’s control when that party has the right, authority, or practical ability, to obtain the documents from a non-party to the action.”) with Bleecker v. Std. Fire Ins. Co., 130 F. Supp. 2d 726, 739 (E.D.N.C. 2000) (“Plaintiff asserts that even if a party does not have the right to require a non-party to produce documents, the party’s practical ability to produce the documents determines whether the defendant has ‘control’ of the document. On the other hand, defendant contends that ‘control’ encompasses a defendant’s legal right to obtain the requested documents. The court agrees with defendant.”). Some courts actually apply the two standards in the alternative. See, e.g., Riddell Sports, Inc. v. Brooks, 158 F.R.D. 555, 558 (S.D.N.Y. 1994) (“If the producing party has the legal right or the practical ability to obtain the documents, then it is deemed to have ‘control,’ even if the documents are actually in the possession of a non-party.”).

⁵⁵ Chevron Corp. v. Salazar, 275 F.R.D. 437, 448–49 (S.D.N.Y. Aug. 3, 2011) (citing to several cases supporting the same proposition).

⁵⁶ Cytogra, Inc. v. IDEXX Laboratories, Inc., CV06-4170PSG(CTX), 2007 WL 5193736 (C.D. Cal. Sept. 21, 2007) *aff’d*, 322 F. App’x 569 (9th Cir. 2009) (party had sufficient control where business documents were stored on remote computer servers).

⁵⁷ See *supra* notes 31–34.

⁵⁸ 730 F. Supp. 2d 860 (N.D. Ill. 2010).

⁵⁹ *Id.* at 865.

⁶⁰ See e.g., Poynter v. Gen. Motors Corp., 476 F. Supp. 2d 854, 857 (E.D. Tenn. 2007) (“As the name suggests, third party spoliation of evidence occurs ‘when a third party destroys evidence that could have been used by a plaintiff against a different defendant in a separate suit.’”); Sillhan v. Allstate Ins. Co., 236 F. Supp. 2d 1303, 1307 (N.D. Fla. 2002) (“This case involves a relatively new tort known as ‘spoliation of evidence’ or ‘destruction of evidence’ . . . [which] arises against a defendant when that defendant breaches a duty to preserve evidence resulting in the destruction of a plaintiff’s cause of action against a third party.”); Foster v. Lawrence Mem’l Hosp., 809 F. Supp. 831, 836 (D. Kan. 1992) (“The tort of spoliation may be based upon negligence or upon intent. In a negligence case, the plaintiff asserts that the defendant negligently destroyed the evidence which impaired the plaintiff’s right to sue a third party tortfeasor.”); Holmes v. Amerex Rent-A-Car, 710 A.2d 846, 848 (D.C. 1998) (holding that the District of Columbia allows “a plaintiff to recover against a defendant who has negligently or recklessly destroyed or allowed to be destroyed evidence that would have assisted the plaintiff in pursuing a claim against a third party.”). Several state courts have also recognized the tort. See discussion in Kolanovic v. Gida, 77 F. Supp. 2d 595, 598–99 (D.N.J. 1999).

⁶¹ *Id.*

⁶² Note also that the direct liability of a cloud computing storage provider to a class of users is at the center of a recent complaint in the case of *Wong v. Dropbox, Inc.*, available at 2011 WL 2492840 (N.D. Cal. 2011). The complaint alleges several common law and statutory claims in response to a bug in the provider’s system that allowed users to access stored files from other users’ accounts.

⁶³ 248 P.3d 1010 (Utah Ct. App. 2011) (plaintiff was awarded default judgment and attorney’s fees for third party’s willful destruction of evidence, including throwing laptops out of windows and running them over with cars).

⁶⁴ See, e.g., Warren Hosp. v. Am. Cas. Co. of Reading, PA, CIV.A. 07-558(JLL), 2009 WL 3074611, at *3 (D.N.J. Sept. 23, 2009) *aff’d sub nom.* 398 F. App’x 800 (3d Cir. 2010) (citing NJ state cases demonstrating that NJ law generally does not recognize employer indemnity actions against employees); Dochniak v. Dominion Mgmt. Services, Inc., CIV. 06-237 JRT/FLN, 2008 WL 906798, at *3 (D. Minn. Apr. 1, 2008) (“Courts in this district have held that the Minnesota indemnification statutes preclude negligence claims by an employer against its employee”).

⁶⁵ See, e.g., Vornado Realty Trust v. Castlton Envtl. Contractors, LLC, 08-CV-04823 DLI JO, 2011 WL 4592800, at *9 (E.D.N.Y. Sept. 30, 2011) (“Under New York law, a claim for indemnification arises only under an express contract of indemnification, or where one defendant is held vicariously liable for the negligence of another through the existence of a relationship between the defendant and the actual wrongdoer, such as that of employee and employer.”) (citation omitted); SeaRiver Mar., Inc. v. Indus. Med. Services, Inc., 983 F. Supp. 1287, 1298 (N.D. Cal. 1997) (“A party who is not at fault but nonetheless is held liable by reason of its relationship to another, such as an employer who is vicariously liable for the acts of his employee, may seek equitable indemnity.”); *In re Boyles*, 22

B.R. 851, 852 (Bankr. N.D. Tex. 1982) (“an employer who is vicariously liable for acts of his employee is entitled to indemnity from that employee”).

⁶⁶ Ellen S. Pryor, *Peculiar Risk in American Tort Law*, 38 PEPP. L. REV. 393, 417 (2011) (“employer indemnity suits against the employee are rare”); Thomas C. Galligan, Jr., *The Dreadful Remnants of the Osceola's Fourth Point*, 34 RUTGERS L.J. 729, 762 (2003) (“employer indemnity or contribution actions against employees are quite rare. Perhaps it is because employers do not think they will actually recover what they have paid or that filing indemnity and contribution actions against employees would discourage qualified people from seeking employment with them.”).

⁶⁷ Press Release, Apple, Inc., iPhone 4S First Weekend Sales Top Four Million (Oct. 17, 2011), *available at* <http://www.apple.com/pr/library/2011/10/17iPhone-4S-First-Weekend-Sales-Top-Four-Million.html>.

⁶⁸ *Id.* Moreover, one survey estimates that iCloud garnered as many as 150 million users. See Lance Whitney, CNet News, Analyst: Apple's iCloud Could See 150 Million Users (June 21, 2011), http://news.cnet.com/8301-13579_3-20072978-37/analyst-apples-icloud-could-see-150-million-users.

⁶⁹ See, e.g., David H. Freedman, *Thinking About Moving to the Cloud? There are Trade-Offs*, N.Y. TIMES, Sept. 22, 2011, at B9.

⁷⁰ Apple, Inc., iCloud Terms and Conditions, <http://www.apple.com/legal/icloud/en/terms.html> (last visited Dec. 8, 2011) (“iTC”) (caps removed).

⁷¹ Consumer Features from Consumer Reports, <http://www.consumerreports.org/cro/electronics-computers/computers-internet/computers/computer-buying-advice/computer-features/computer-features.htm> (last visited Dec. 8, 2011).

⁷² Farhad Manjoo, Slate, Flight of the Desktops: Soon There will be no Reason to Have a Big, Boxy Computer on Your Desk (June 18, 2010), http://www.slate.com/articles/technology/technology/2010/06/flight_of_the_desktops.html.

⁷³ See *id.*

⁷⁴ IPASS, INC., THE IPASS MOBILE WORKFORCE REPORT 10 (2010), <http://www3.ipass.com/elqNow/elqRedir.htm?ref=http://www3.ipass.com/wp-content/uploads/2010/11/Mobile-Workforce-Report-November-2010.pdf>.

⁷⁵ Compare The Nielson Company, With Smartphone Adoption on the Rise, Opportunity for Marketers is Calling (Sept. 15, 2009), http://blog.nielsen.com/nielsenwire/online_mobile/with-smartphone-adoption-on-the-rise-opportunity-for-marketers-is-calling, with The Nielson Company, Mobile Snapshot: Smartphones Now 28% of U.S. Cellphone Market (Nov. 1, 2010), http://blog.nielsen.com/nielsenwire/online_mobile/mobile-snapshot-smartphones-now-28-of-u-s-cellphone-market, with The Nielson Company, In U.S. Market, New Smartphone Buyers Increasingly Embracing Android (Sept. 26, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/in-u-s-market-new-smartphone-buyers-increasingly-embracing-android (smartphone penetration of mobile market has risen from 10% in 2008 to 17% in 2009 to 28% in 2010 and to 43% in 2011).

⁷⁶ See, e.g. *A Brief History of Wi-Fi*, ECONOMIST, June 10, 2004, *available at* <http://www.economist.com/node/2724397>; CISCO SYSTEMS, INC., THE FUTURE OF HOTSPOTS: MAKING WI-FI AS SECURE AND EASY TO USE AS CELLULAR 1 (2011), *available at* http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns673/white_paper_c11-649337.pdf (“According to the Wi-Fi Alliance, about 200 million households use Wi-Fi networks and there are about 750,000 Wi-Fi hotspots worldwide. Wi-Fi is used by over 700 million people and there are about 800 million new Wi-Fi devices every year.”).

⁷⁷ See e.g., AARON SMITH, PEW RESEARCH CENTER, 35% OF AMERICAN ADULTS OWN A SMARTPHONE: ONE QUARTER OF SMARTPHONE OWNERS USE THEIR PHONE FOR MOST OF THEIR ONLINE BROWSING 3 (2011), *available at* http://www.pewinternet.org/~media/Files/Reports/2011/PIP_Smartphones.pdf (“When asked what device they normally use to access the internet, 25% of smartphone owners say that they mostly go online using their phone, rather than with a computer.”).

⁷⁸ See, e.g., Apple – iPod Touch – it’s Fun-Filled and Feature-Packed, <http://www.apple.com/ipodtouch/features> (last visited Dec. 8, 2011).

⁷⁹ Apple’s iWork suite, which includes software to create documents, spreadsheets, and presentations, can be used on PCs, laptops, iPods, iPhones, and iPads. See Apple – iWork – Documents, Spreadsheets, and Presentations. The Mac Way., <http://www.apple.com/iwork> (last visited Dec. 8, 2011).

⁸⁰ These devices are all equipped with calendar, e-mail, and contact list functionality. See Apple, Inc., Calendar, Mail, and Contacts, <http://www.apple.com/icloud/features/calendar-mail-contacts.html> (last visited Dec. 8, 2011).

⁸¹ Note that, of the different types of iPods, only the iPod Touch has internet connectivity.

⁸² See generally Apple's website (<http://www.apple.com>) for product descriptions.

⁸³ While some cloud computing competitors are involved in computing devices, they do not have the same breadth or history. For example, Google's involvement has been limited to developing its Android operating system for smartphones and tablets since late 2007. See Press Release, Open Handset Alliance, Industry Leaders Announce Open Platform for Mobile Devices (Nov. 5, 2007), available at http://www.openhandsetalliance.com/press_110507.html. Amazon's Kindle, which was introduced in November 2007, has only recently expanded its product line and grown from merely an eReader to a more comprehensive computing device. See Press Release, Amazon.com, Inc., Introducing Amazon Kindle (Nov. 19, 2007), available at <http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1079388>; Press Release, Amazon.com, Inc., Introducing the All-New Kindle Family: Four New Kindles, Four Amazing Price Points (Sept. 28, 2011), available at <http://phx.corporate-ir.net/phoenix.zhtml?c=176060&p=irol-newsArticle&ID=1610968>. Microsoft has offered cloud storage for Microsoft Office files since October of 2010, but, similarly to Google, has limited its mobile computing penetration to operating systems. See Press Release, Microsoft, Microsoft Announces Office 365 (Oct. 19, 2010), available at <http://www.microsoft.com/presspass/press/2010/oct10/10-19office365.mspx>; Windows 8 Makes Microsoft a Tablet Contender Against Android, Apple – Forbes (Sept. 15, 2011), <http://www.forbes.com/sites/greatspeculations/2011/09/15/windows-8-makes-microsoft-a-tablet-contender-against-android-apple>.

⁸⁴ Apple, Inc., What is iCloud?, <http://www.apple.com/icloud/what-is.html> (last visited Dec. 8, 2011) (emphasis added).

⁸⁵ *Id.* (emphasis added).

⁸⁶ Apple, Inc., Documents in the Cloud, <http://www.apple.com/icloud/features/documents.html> (last visited Dec. 8, 2011) (emphasis added).

⁸⁷ Garrett Sloane, Apple Hits 250M Units Sold; Next 250 Harder, N.Y. POST, July 30, 2012, http://www.nypost.com/p/news/business/iphone_euphoria_OE0quy8kIM6RGQYytDC9IK.

⁸⁸ Ian Paul, Apple Earnings Disappoint, But iPad Sales Continue to Surge, PCWORLD, July 25, 2012, http://www.pcmag.com/article/259829/apple_earnings_disappoint_but_ipad_sales_continue_to_surge.html.

⁸⁹ Complaint at ¶¶ 15, 16, 18, Apple Inc. v. Samsung Electronics Co., Ltd, 768 F. Supp. 2d 1040 (N.D. Cal. 2011), available at 2011 WL 1461508 or <http://www.apple.com/pr/pdf/110415samsungcomplaint.pdf>.

⁹⁰ Ed Bott, Second Source Confirms: 1 in 100 Macs are Infected by Flashback, ZDNet, Apr. 6, 2012, <http://www.zdnet.com/blog/bott/second-source-confirms-1-in-100-macs-are-infected-by-flashback/4737>.

⁹¹ Nick Wingfield, *A Corporate Yen for iTools*, N.Y. TIMES, Nov. 16, 2011, at B1.

⁹² Rachel King & Adam Satariano, Apple Gets Corporate Sales Backup at Unisys, BUSINESSWEEK, Oct. 25, 2010, http://www.businessweek.com/technology/content/oct2010/tc20101026_138220.htm.

⁹³ Brier Dudley, *Apple iPhone Liveblog Roundup: New iPads, iCloud, iPhone 4S*, SEATTLE TIMES, Oct. 4, 2011, http://seattletimes.nwsource.com/html/technologybrierdudleysblog/2016401085_apple_iphone_5.html.

⁹⁴ Peter Pachal, *Apple iPad: Stronger than Ever*, PC MAG., October 19, 2011, <http://www.pcmag.com/article2/0,2817,2394928,00.asp#fbid=xVdmFvmb8zY>.

⁹⁵ Press Release, Techaisle, Small Business' Early iPad Adoption Shows Promise for Tablet PCs, says Techaisle (Nov. 4, 2010), available at <http://www.techaisle.com/prsmbipadadoption.html>; see also JULIO OJEDA-ZAPATA, IPAD MEANS BUSINESS: HOW APPLE'S TABLET COMPUTER IS CHANGING THE WORK WORLD, 57–80 (2010) (describing iPad adoption by the following companies: West Point Thoroughbreds, Ruane Attorneys-at-Law, Wells Fargo, Advanced Cosmetic Surgery and Laser Center, SageView Advisory Group, Arhaus Furniture, D7 Consulting, Studio2, Scale Computing, TechNosis, Markley Enterprises, United Insurance Finance Company, Innovative Metabolic Solutions, and Quality Tool).

⁹⁶ Ben Worthen, *Businesses Add iPads to Their Briefcases*, WALL ST. J., Aug. 24, 2010, at B5; Martha C. White, *With the iPad, Apple may Just Revolutionize Medicine*, WASH. POST, Apr. 11, 2010, <http://www.washingtonpost.com/wp-dyn/content/article/2010/04/09/AR2010040906341.html>; Miguel Helft, *After iPad's Head Start, Rival Tablets Are Poised to Flood Offices*, N.Y. TIMES, Feb. 21, 2011, at B1.

⁹⁷ Helft, *supra* note 94.

⁹⁸ Verne G. Kopytoff, *More Offices Let Workers Choose Their Own Devices*, N.Y. TIMES, Sept. 23, 2011, at B1.

⁹⁹ Dan Frommer, Business Insider, Here's How Apple's iPad Is Invading The Business World (Oct. 1, 2010), http://articles.businessinsider.com/2010-10-01/tech/30084383_1_ipad-text-message-device.

¹⁰⁰ GOOD TECHNOLOGY, GOOD TECHNOLOGY DEVICE ACTIVATIONS REPORT Q2 2011: IPADS DRIVE IOS DOMINANCE IN THE ENTERPRISE 12 (2011), available at http://www.good.com/resources/Good_Data_Q2_2011.pdf.

¹⁰¹ Emre Peker, Bloomberg, JPMorgan Gives Bankers iPads in ‘Clear and Present Danger’ to RIM (Nov. 30 210), <http://www.bloomberg.com/news/2010-11-30/jpmorgan-gives-its-investment-bankers-ipads-in-challenge-to-rim-blackberry.html>.

¹⁰² Sarah Yin, *How the iPad is Emerging as a Business Tool*, PC MAG., Apr. 11, 2011, <http://www.pcmag.com/article2/0,2817,2382952,00.asp#fbid=xVdmFvmb8zY>.

¹⁰³ Joel Mathis, MacWorld, Mercedes-Benz Financial Pushes iPad Program Nationwide (Oct. 5, 2010), http://www.macworld.com/article/154592/2010/10/mercedes_ipad.html.

¹⁰⁴ Helft, *supra* note 94.

¹⁰⁵ *Jargon buster: What is consumerisation?*, THE HP BLOG HUB, (Dec. 1, 2011, 7:13 AM),

<http://h30507.www3.hp.com/t5/Business-Answers/Jargon-buster-What-is-consumerisation/ba-p/103061>

(“Consumerization is a stable neologism that describes the trend for new information technology to emerge first in the consumer market and then spread into business organizations, resulting in the convergence of the IT and consumer electronics industries, and a shift in IT innovation from large businesses to the home.”).

¹⁰⁶ Oren Tversky, Gigaom, The Democratization of the Enterprise (Aug. 14, 2011), <http://gigaom.com/cloud/the-democratization-of-the-enterprise>.

¹⁰⁷ Kopytoff, *supra* note 96.

¹⁰⁸ *Id.*; Alan Drummer, Symantec Corporation, The “Consumerization” of IT: What Should You Resist? Or Embrace? (2009), http://www.symantec.com/business/ciodigest/article.jsp?aid=april09_solutions.

¹⁰⁹ Press Release, The NPD Group, Apple Owners Nearly 40 Percent More Interested in the iPad than Non-Apple Owners, According to NPD (Mar. 26, 2010), https://www.npd.com/press/releases/press_100326.html; Chloe Albanesius, *Report: Apple Boasts 89 Percent Retention Rate, RIM Users Less Loyal*, PC MAG., Sept. 23, 2011, <http://www.pcmag.com/article2/0,2817,2393452,00.asp#fbid=xVdmFvmb8zY>.

¹¹⁰ John Hazard, ZDNet, Apple's iPad is Winning the Enterprise Tablet Race Without Even Trying (Feb. 16, 2011), <http://www.zdnet.com/blog/btl/apples-ipad-is-winning-the-enterprise-tablet-race-without-even-trying/44932>.

¹¹¹ Nathan Clevenger, InfoWorld, How the iPad will Change IT Forever: Apple's Tablet is Pushing the ‘Consumerization of IT’ Trend in a Way that IT Can't Stop -- and Doesn't Need to (Aug. 2, 2011), <http://www.infoworld.com/t/it-management/how-the-ipad-will-change-it-forever-166948>.

¹¹² Apple – iCloud Stores Your Content and Pushes it to Your Devices, <http://www.apple.com/icloud/what-is.html> (last visited Dec. 8, 2011).

¹¹³ Apple – iCloud – Keep the Same Documents up to Date Everywhere, <http://www.apple.com/icloud/features/documents.html> (last visited Dec. 8, 2011) (a document stored on iCloud “automatically appears on all your iOS devices, ready for you to review, edit, or present.”).

¹¹⁴ See Apple – iOS 5 – See New Features Included in iOS 5, <http://www.apple.com/ios/features.html> (last visited Dec. 8, 2011).

¹¹⁵ David Pogue, *A Look at Apple's iCloud*, N.Y. TIMES, Oct. 13, 2011, <http://pogue.blogs.nytimes.com/2011/10/13/a-look-at-icloud>.

¹¹⁶ *Id.*; Apple – iCloud – Keep the Same Documents up to Date Everywhere, <http://www.apple.com/icloud/features/documents.html> (last visited Dec. 8, 2011).

¹¹⁷ See *supra* note 9.

¹¹⁸ See *supra* notes 2–4.

¹¹⁹ See *supra* note 38.

¹²⁰ *Cyntegra*, 2007 WL 5193736, at *5 (“A contractual relationship with a third-party entity provides, at a minimum, an obligation to make reasonable inquiry of the third party entity for the data at issue.”).

¹²¹ iTC, *supra* note 70.

¹²² *Id.*

¹²³ *Id.* (emphasis added).

¹²⁴ According to the Sedona Principles, “[m]etadata includes information about the document or file that is recorded by the computer to assist in storing and retrieving the document or file,” and specifically, “hidden text, formatting codes, formulae, and other information associated with the file.” SEDONA PRINCIPLES, at 3, cmt. 12.a. Moreover,

It is common for electronic information to be migrated to a number of different applications and formats in the ordinary course of business, particularly if the information is archived for long-term storage. Routine migration will likely result in the loss or alteration of some elements of metadata associated with the native application, and the addition of new elements.”

Id. at 8.

¹²⁵ iTC. (emphasis added).

¹²⁶ See *id.*, cmt. 9.a, princ. 12 (“production should be made ... taking into account the need to produce reasonably accessible metadata that will enable the receiving party to have the same ability to access, search, and display the information as the producing party where appropriate or necessary in light of the nature of the information and the needs of the case.”).

¹²⁷ *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640 (D. Kan. 2005).

¹²⁸ FED. R. CIV. P. 34(b)(2)(E)(i) requires that parties “produce documents as they are kept in the usual course of business must organize and label them to correspond to the categories in the request.”

¹²⁹ *Williams*, 230 F.R.D. at 652; see also *Allen v. Woodford*, CVF051104OWWLJO, 2007 WL 309943, at *2 (E.D. Cal. Jan. 30, 2007) (Defendants “should be compelled to conduct a thorough electronic review and to produce all responsive documents in electronic format, along with any metadata”); *In re Vioxx Prod. Liab. Litig.*, MDL 1657, 2005 WL 756742, at *3 (E.D. La. Feb. 18, 2005) (“‘Documents, data, and tangible things’ is to be interpreted broadly to include ... [i]nformation that serves to identify, locate, or link such material, such as file inventories, file folders, indices, and metadata.”).

¹³⁰ See, e.g., *In re Telxon Corp. Sec. Litig.*, 5:98CV2876, 2004 WL 3192729, at *34–35 (N.D. Ohio July 16, 2004).

¹³¹ iTC, *supra* note 70. Those circumstances include:

(a) violations of this Agreement or any other policies or guidelines that are referenced herein and/or posted on the Service; (b) a request by you to cancel or terminate your Account; (c) a request and/or order from law enforcement, a judicial body, or other government agency; (d) where provision of the Service to you is or may become unlawful; (e) unexpected technical or security issues or problems; (f) your participation in fraudulent or illegal activities; or (g) failure to pay any fees owed by you in relation to the Service.

Id.

¹³² *Id.*

¹³³ *Cyntegra, Inc. v. IDEXX Laboratories*, No. 06-4170, 2007 WL 5193736 (C.D. Cal. Sept. 21, 2007).

¹³⁴ *Id.* at *1.

¹³⁵ *Id.* at *1, *5.

¹³⁶ *Id.* at *5.

¹³⁷ *Id.* at *6.

¹³⁸ See iTC, *supra* notes 129, 130.

¹³⁹ iTC, *supra* note 70.

¹⁴⁰ Editorial, *The Cloud Darkens*, N.Y. TIMES, June 30, 2011, at A26, available at <http://www.nytimes.com/2011/06/30/opinion/30thu1.html>; see also *supra* note 62 (a lawsuit has already been filed in response).

¹⁴¹ *The Cloud Darkens*, *supra* note 140.

¹⁴² iTC, *supra* note 70.

¹⁴³ *Id.* (caps removed).

¹⁴⁴ *Id.* (emphasis added).

¹⁴⁵ *Id.*

¹⁴⁶ See, e.g., *Schwan's Sales Enter., Inc. v. SIG Pack, Inc.*, 476 F.3d 594, 598 (8th Cir. 2007); *Fin. One Pub. Co. Ltd. v. Lehman Bros. Special Fin., Inc.*, 414 F.3d 325, 332 (2d Cir. 2005) (“The validity of a contractual choice-of-law clause is a threshold question that must be decided not under the law specified in the clause, but under the relevant forum's choice-of-law rules governing the effectiveness of such clauses.”); see also RESTATEMENT (SECOND) OF CONFLICTS OF LAW § 186 cmt. b.

¹⁴⁷ Gillian Lester & Elizabeth Ryan, *Choice of Law and Employee Restrictive Covenants: An American Perspective*, 31 COMP. LAB. L. & POL'Y J. 389, 397 (2010) (“In general, courts defer to choice of law clauses because they are presumed to represent the express intention of the parties.”).

¹⁴⁸ See, e.g., RESTATEMENT (SECOND) OF CONFLICTS OF LAW § 187 (Law of the State Chosen by the Parties).

¹⁴⁹ CAL. CIV. CODE § 1668.

¹⁵⁰ *Capri v. L.A. Fitness Int'l, LLC*, 39 Cal. Rptr. 3d 425, 429 (Cal. Ct. App. 2006) (citation omitted).

¹⁵¹ See, e.g., *City of Santa Barbara v. Superior Court*, 161 P.3d 1095, 1115 (Cal. 2007).

¹⁵² *Reudy v. Clear Channel Outdoors, Inc.*, 693 F. Supp. 2d 1091, 1115 (N.D. Cal. 2010) *aff'd sub nom.* *Reudy v. CBS Corp.*, 430 F.App'x 568 (9th Cir. 2011).

¹⁵³ *Tunkl v. Regents of Univ. of Cal.*, 383 P.2d 441 (Cal. 1963).

¹⁵⁴ *Id.* at 444–46.

¹⁵⁵ *Id.* at 441–42.

¹⁵⁶ *Id.* at 442.

¹⁵⁷ *Id.* at 444.

¹⁵⁸ *Id.* at 444–46; *see also Reudy*, 693 F. Supp. 2d at 1115.

¹⁵⁹ *Tunkl*, 383 P.2d at 447.

¹⁶⁰ *iTC*, *supra* note 70. The provision “Apple's failure to use reasonable skill and due care” is synonymous with an analysis of negligence.

¹⁶¹ *Guivi v. Spectrum Club Holding Co.*, B222639, 2011 WL 1589117, at *8 (Cal. Ct. App. Apr. 28, 2011) (citation omitted).

¹⁶² (1) Remote ESI storage is not generally thought suitable for public regulation: “Types of services thought to be subject to public regulation have included common carriers, hospitals and doctors, public utilities, innkeepers, public warehousemen, employers and services involving extra-hazardous activities.” *Hoot Winc, L.L.C. v. RSM McGladrey Fin. Process Outsourcing, LLC*, 08CV1559 BTM(WMC), 2009 WL 3805212, at *3 (S.D. Cal. Nov. 12, 2009) (citation omitted). (2) Remote ESI storage is not a service of great importance to the public, which is often a matter of practical necessity for some members of the public: “medical, legal, housing, transportation or similar services which must necessarily be utilized by the general public” have satisfied this factor. *Hulsey v. Elsinore Parachute Ctr.*, 214 Cal. Rptr. 194, 199 (Cal. Ct. App. 1985).

¹⁶³ In fact, assumedly as a result of indicating interest in iCloud and entering an email address on the Apple website, the author received an email on October 22, 2011 from Apple with the subject “Get iOS 5 and iCloud for your iPhone, iPad, and iPod Touch.”

¹⁶⁴ *CAZA Drilling (California), Inc. v. TEG Oil & Gas U.S.A., Inc.*, 48 Cal. Rptr. 3d 271, 283–84 (Cal. Ct. App. 2006) (citation omitted).

¹⁶⁵ A contract of adhesion is characterized as “a standardized contract, which, imposed and drafted by a party of superior bargaining strength, relegates to the subscribing party only the opportunity to adhere to the contract or reject it.” *Lanigan v. City of Los Angeles*, B228686, 2011 WL 4552533, at *9 (Cal. Ct. App. Oct. 4, 2011) (citation omitted).

¹⁶⁶ *See infra* Part III.A (discussing possibility of negotiations).

¹⁶⁷ Susan A. Berson, *Safe in the Cloud? Online Service Risks Need Care and Coverage*, ABA J., Nov. 1, 2011, available at

http://www.abajournal.com/magazine/article/safe_in_the_cloud_online_service_risks_need_care_and_coverage (“‘Most big cloud providers are limited as to how much they will change contractually because law firms are small potatoes for them,’ says Tanner [an attorney specializing in business records management]. ‘Even if the cloud company is willing to change the contract ... the underlying provider may not be willing to make contractual adjustments unless you are a huge customer.’”).

¹⁶⁸ *Guivi v. Spectrum Club Holding Co.*, B222639, 2011 WL 1589117 (Cal. Ct. App. Apr. 28, 2011).

¹⁶⁹ *Id.* at *1, *4–5.

¹⁷⁰ *Id.* at *6.

¹⁷¹ *Id.*

¹⁷² *Id.*

¹⁷³ *Id.*

¹⁷⁴ *Magliocco v. Am. Locker Co., Inc.*, 239 Cal. Rptr. 497 (Ct. App. 1987).

¹⁷⁵ *Id.* at 499.

¹⁷⁶ *Id.* at 503.

¹⁷⁷ *See supra* Part II.B.

¹⁷⁸ For example, according to the legal head of Google’s European enterprise, Cindy Yip, “[i]n a cloud context, SLAs [Service Level Agreements] tend not to be negotiable” as “[i]t wouldn’t be practical for a cloud service provider to meet the demands of one customer.” David Swabey, *Information Age, Don’t Try to Negotiate Special Treatment From Cloud Providers*, Warns Google (Oct. 21, 2010), <http://www.information-age.com/channels/it-services/news/1292673/dont-try-to-negotiate-special-treatment-from-cloud-providers-warns-google.html>; *see also* Press Release, Gartner, Gartner Highlights IT Procurement Best Practices to Reduce Risk in Cloud Contracts (May 19, 2011), <http://www.gartner.com/it/page.jsp?id=1689914> (according to “Alexa Bona, research vice president at

Gartner[,] “[m]any cloud providers appear reluctant to negotiate contracts, as the premise of their core model is a highly leveraged approach. The starting point contractually often favors the vendor, resulting in a potential misalignment with user requirements.”).

¹⁷⁹ See, e.g., *Consensus Assessments Initiative Questionnaire*, CONSENSUS ASSESSMENTS INITIATIVE: CLOUD SECURITY ALLIANCE (Dec. 8, 2011), <https://cloudsecurityalliance.org/research/initiatives/cai> (offering an outline of issues to address when negotiating a cloud computing service agreement); Alexa Bona & Frank Ridder, *IT Procurement Best Practice: Nine Contractual Terms to Reduce Risk in Cloud Contracts* (Dec. 8, 2011), <http://www.gartner.com/DisplayDocument?ref=clientFriendlyUrl&id=1599115>.

¹⁸⁰ See, e.g., Thomas J. Trappier, *If It's in the Cloud, Get it on Paper: Cloud Computing Contract Issues*, EDUCAUSE REVIEW (Jun. 24, 2010), <http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/IfltsintheCloudGetItOnPaperClo/206532> (describing numerous cloud contract provisions negotiated by university clients).

¹⁸¹ See *Lanigan v. City of Los Angeles*, B228686, 2011 WL 4552533, at *9 (Cal. Ct. App. Oct. 4, 2011).

¹⁸² See GOOGLE APPS FOR BUSINESS, <http://www.google.com/apps/intl/en/business/index.html> (last visited Sep. 16, 2012).

¹⁸³ *Google Apps for Business (Online) Agreement*, GOOGLE APPS §§ 12, 13.1, 13.2, http://www.google.com/apps/intl/en/terms/standard_terms.html (last visited Sep. 16, 2012) (caps removed).

¹⁸⁴ GOOGLE APPS FOR BUSINESS, <http://www.google.com/apps/intl/en/business/index.html> (last visited Sep. 16, 2012).

¹⁸⁵ See IT'S TIME TO GO GOOGLE, <http://www.google.com/apps/intl/en/customers/index.html#tab6> (last visited Sep. 16, 2012) (listing the various governmental entities that have adopted Google Apps).

¹⁸⁶ While data indicating the number of businesses that have negotiated Google Apps Terms of Service is not available, it would be beyond reason to expect that Google has independently negotiated its terms with anything close to 4 million different businesses.

¹⁸⁷ See Sarno, *supra* note 17.

¹⁸⁸ IT'S TIME TO GO GOOGLE, *supra* note 185; knowledge of these negotiations is also premised partly on the author's conversations with Kate DeSimone, counsel for the City of Pittsburgh's Information Systems Department. Telephone Interview with Kate DeSimone, Counsel, City of Pittsburgh Information Systems Department, in Pittsburgh, Pa. (Nov. 28, 2011).

¹⁸⁹ CITY OF LOS ANGELES, PROFESSIONAL SERVICES CONTRACT BETWEEN THE CITY OF LOS ANGELES AND COMPUTER SCIENCE CORP. FOR THE SAAS E-MAIL AND COLLABORATION SOLUTION (SECS) (2009), *available at* http://clkrep.lacity.org/onlinecontracts/2009/C-116359_c_11-20-09.pdf [hereinafter L.A. CONTRACT].

¹⁹⁰ *Id.* at Contract Summary Sheet; see also Sarno, *supra* note 17.

¹⁹¹ L.A. CONTRACT, *supra* note 189 at app. B.

¹⁹² L.A. CONTRACT, *supra* note 189 at app. J.

¹⁹³ L.A. CONTRACT, *supra* note 189 at app. B.

¹⁹⁴ L.A. CONTRACT, *supra* note 189 at § 15.1.1 (caps removed and emphasis added to indicate changes from standard terms).

¹⁹⁵ L.A. CONTRACT, *supra* note 189 at § 15.1.2.

¹⁹⁶ L.A. CONTRACT, *supra* note 189 at § 15.5.3.

¹⁹⁷ Compare L.A. CONTRACT, *supra* note 189 at app. J, with *Google Apps for Business (Online) Agreement*, *supra* note 183 at § 12.

¹⁹⁸ Compare L.A. CONTRACT, *supra* note 189 at app. J.1 § 13.2.4, with L.A. CONTRACT, *supra* note 189 at § 15.5.3. Note that the extent that these seemingly inconsistent provisions can be reconciled is outside the scope of this paper.

¹⁹⁹ Compare L.A. CONTRACT, *supra* note 189 at app. J.1 § 14.1 (caps removed), with *Google Apps for Business (Online) Agreement*, *supra* note 183 at § 12.

²⁰⁰ L.A. CONTRACT, *supra* note 189 at app. J.1 § 14.2.

²⁰¹ See David Navetta, *What's in Google's SaaS Contract with the City of Los Angeles? Part Three*, INFOGROUP (June 23, 2010), <http://www.infolawgroup.com/2010/06/articles/cloud-computing-1/whats-in-googles-saas-contract-with-the-city-of-los-angeles-part-three> (providing a comprehensive analysis of the L.A. CONTRACT).

²⁰² DASTON PROFESSIONAL SERVICES AGREEMENT (2011), *available at* <http://www.openbookpittsburgh.com/Contracts.aspx?vendor=daston&vtype=B> [hereinafter PITTSBURGH CONTRACT].

²⁰³ Scott McIntyre, *The Steel City Goes Google*, GOOGLE INC. (July 18, 2011), <http://googleenterprise.blogspot.com/2011/07/steel-city-goes-google.html>.

²⁰⁴ PITTSBURGH CONTRACT, *supra* note 202 at 1–3.

²⁰⁵ Compare L.A. CONTRACT, *supra* note 189 at app. b with PITTSBURGH CONTRACT, *supra* note 202 at exhibit A.

²⁰⁶ And in fact, they did consider e-discovery issues. See Brian Heaton, *Pittsburgh's City Government to Outsource E-Mail*, GOVERNMENT TECHNOLOGY (July 20, 2011), <http://www.govtech.com/e-government/Pittsburghs-City-Government-to-Outsource-E-Mail.html> (“E-discovery is another area Stern [Pittsburgh CIO] felt would be streamlined by moving to a hosted e-mail solution. He said that the ability to store, retrieve and search documents, e-mails and other communications was a ‘non-negotiable issue’ when considering cloud providers.”).

²⁰⁷ PITTSBURGH CONTRACT, *supra* note 202 at exhibit A §§ 3.4, 3.5.

²⁰⁸ Compare PITTSBURGH CONTRACT, *supra* note 202 at add. § 15.1, with *Google Apps for Business (Online) Agreement*, *supra* note 183 at § 12.1, and L.A. CONTRACT *supra* note 189 at app. J (caps removed).

²⁰⁹ PITTSBURGH CONTRACT, *supra* note 202 at add. § 15.2; See L.A. CONTRACT, *supra* note 189 at app. J.

²¹⁰ PITTSBURGH CONTRACT, *supra* note 202 at add. § 14.2.

²¹¹ Compare PITTSBURGH CONTRACT, *supra* note 202, with L.A. CONTRACT, *supra* note 189.

²¹² Federal Information Security Management Act, 44 U.S.C. §§ 3541–3549.

²¹³ 44 U.S.C. § 3541(3).

²¹⁴ 44 U.S.C. § 3543(a)(1).

²¹⁵ 44 U.S.C. § 3543(a)(2)(A), (B).

²¹⁶ See NAT'L INST. OF STANDARDS & TECH. SECURITY DIVISION COMPUTER SECURITY RES. CTR., <http://csrc.nist.gov/groups/SMA/fisma/index.html> (last visited Dec. 8, 2011); see also, e.g., NIST, U.S. DEP'T. OF COMMERCE, RECOMMENDED SECURITY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS (2010), available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

²¹⁷ See NAT'L INST. OF STANDARDS & TECH., NSIT CLOUD COMPUTING PROGRAM, <http://www.nist.gov/itl/cloud> (last visited Dec. 8, 2011).

²¹⁸ GOOGLE APPS FOR GOVERNMENT, <http://www.google.com/apps/intl/en/government/trust.html> (last visited Dec. 8, 2011).

²¹⁹ Susie Adams, *USDA Awards FISMA Certification for Microsoft's Business Productivity Online Suite – Federal*, MICROSOFT CORP. (Apr. 20, 2011), <http://www.microsoft.com/government/en-us/federal/futurefed/Pages/details.aspx?USDA-Awards-FISMA-Certification-for-Microsoft%E2%80%99s-Business-Productivity-Online-Suite-%28BPOS%29---Federal&blogid=125>.

²²⁰ *Amazon Cloud Adds FISMA Moderate to Security Certifications*, GOV. TECH. (Sept. 15, 2011), <http://www.govtech.com/security/Amazon-Cloud-Adds-FISMA-Moderate-Security-Certifications.html>.

²²¹ PITTSBURGH CONTRACT, *supra* note 202 at add. § 1.3.

²²² *Google Apps for Business (Online) Agreement*, *supra* note 183 at § 1.1.

²²³ It is worth noting that Apple has actually offered cloud computing services as far back as January 2000 through their iTools product. iTools has since been reconfigured and rebranded several times, but has only recently become widely successful in its current form as iCloud. See Corey Bohon, *The History of Apple's Cloud Services*, MACLIFE (June 7, 2011), http://www.maclife.com/article/gallery/history_apples_cloud_services.

²²⁴ See *supra* note 176.

²²⁵ See *supra* Part II.A.

²²⁶ See *supra* Part II.B.

²²⁷ Cat Casey, *iCloud: E-Discovery Practitioner Concerns*, HUDSON LEGAL (Nov. 21, 2011), <http://hudsonlegalblog.com/e-discovery/icloud-e-discovery-practitioner-concerns.html>.

²²⁸ See Gavin Clarke, *Apple's iCloud Runs on Microsoft and Amazon Services: Who Says Azure isn't Cool and Trendy Now*, THE REGISTER (Sept. 2, 2011), http://www.theregister.co.uk/2011/09/02/icloud_runs_on_microsoft_azure_and_amazon.

²²⁹ Wingfield, *supra* note 91.

²³⁰ See *Google Apps for Business (Online) Agreement*, *supra* note 183; c.f. *Document Deletion and Recovery Policy*, GOOGLE DOCS <http://docs.google.com/support/bin/answer.py?hl=en&answer=1704883&topic=1361271> (last visited Dec. 8, 2011).

²³¹ See, e.g., *Cloud Terms of Service*, RACKSPACE CLOUD LEGAL, <http://www.rackspace.com/cloud/legal/> (last updated Aug. 30, 2012).

²³² Clarke, *supra* note 228.

²³³ See, e.g., JAY HEISER & MARK NOCELETT, GARTNER, INC., ASSESSING THE SECURITY RISKS OF CLOUD COMPUTING (2008), available at <http://cloud.ctrls.in/files/assessing-the-security-risks.pdf>; ROBERT GELLMAN, PRIVACY IN THE CLOUDS: RISKS TO PRIVACY AND CONFIDENTIALITY FROM CLOUD COMPUTING (2009), available at http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

²³⁴ See, e.g., George Lawton, *Cloud Computing in 2011: What's on Tap?*, TECHTARGET (Dec. 2010), <http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-in-2011-Whats-on-tap>.