Leveraging Cloud technology to lower costs & improve security in the **legal industry.**

Every part of our personal and professional lives is being impacted by the transition to the Cloud. As we once outsourced each of our other utility services to large private enterprise; and created professions dedicated to specialist areas of knowledge, we are now seeing this transition in respect of data and the computing systems that work with it. Here we tackle the impact of utility computing in the legal sector.

Introduction

The year 2007 saw the world change, though few would have appreciated it at the time. For those who have forgotten, it was in 2007 that Apple Computers Inc. launched the first generation iPhone. It was not the first "smart phone" but it was the first of a new breed, not designed for specific business needs, but designed for the masses and with the Cloud firmly at its core. Then in 2010 it happened again, this time with the iPad. Once again, Apple didn't invent the tablet, nor would many argue did they perfect it, but they did make it acceptable to the masses. These two commercial product launches signalled the death of traditional IT and the permanent shift to a Cloud-based utility computing model.

Just as our other utilities; water, fuel & electricity were once all produced on-site by the consumer, but are now considered so remote to the consumer that we scarcely even bother to ensure we're getting the best price; so too will be the fate of computing. However there's another parallel to another cultural shift occurring at the same time, that of specialist knowledge. Just as the legal industry itself was born out of the explosive growth in knowledge specific to its field, the IT industry has in recent years seen an equal if not more dramatic growth in its body of knowledge; it too is beginning to be the realm of a select highly-educated and experienced few.

We know from history that resisting these kinds of tectonic shifts is futile, so the question becomes how can you be one of the winners and avoid being crushed by the shifting plates of our world?

Contents

Description of **Cloud Services**

Many people today mistakenly attribute the Cloud to be synonymous with the Internet, or to large-scale computing infrastructure. In truth, the Cloud is neither of these things; it's simply clever marketing around the same concept, just like any other public utility. It says "show me what this does for me and not how it does it" in just the same way as we would rarely question exactly which power plant or technology is being used to power our homes and offices. It's important to understand each of the terms as it relates to the user.

Internet is by its very definition an inter-network. A network created as a result of several other networks connecting together. The Internet is not just one specific network but the result of the choices of the world's network providers in allowing the free movement of data between their networks. This is why issues such as net neutrality and supposed "Internet Regulation" are so important but also often so futile. The Internet does not exist, so how would anyone purport to regulate it? What we're really talking about is regulating the behaviours of individuals and companies who have, voluntarily, agreed to create a global communications system.

We can now understand that just as with the electrical system, where our national grids (and even often our sub-national, regional grids) have very little interconnectedness but still represent a public utility; the utility nature of any 'Cloud' computing services does not rely on the Internet. The fact that our data 'grid' is better connected internationally than the grid we use for electricity or natural gas is an irrelevance. The Cloud is not synonymous with the Internet, and in-fact the notion that you can or should access a computing service which is not provided locally, but is from some distance away and must traverse several independent, private networks via the informal agreement that is the Internet becomes questionable at best.

The fundamental concept of Cloud services in all their forms is that it is cheaper, safer and ultimately easier to consume than the ever increasing volume and complexity of computing needs from a specialised service provider. This is as true in computing as it is in legal (law firms) or finance (banks). It simply makes no sense to continue in a pure DIY fashion when it comes to your computing needs.

If we look closer at some of the layers of computing which can be easily outsourced to a Cloud provider we should consider software (Software-as-a-Service or SaaS), infrastructure (Infrastructure-as-a-Service or IaaS), and the newest layer, desktops (Desktops-as-a-Service or DaaS).

Hosted Software

The first and most obvious element of outsourced or Cloud IT is software. Early in the dot-com days of the 1990's we had numerous businesses setup under the banner of Application Service Providers. The model was the same, the marketing just hadn't caught up yet, but this was Cloud and SaaS. One of the most easily recognised of these dot-com era companies, still with us today is SalesForce.com. Founded in 1999, they adopted the mantra of "no software". A curious concept for a software company! Still the point was sound, they wanted businesses to understand that it was no-longer necessary to purchase, download and install software in order to gain the business benefits of said software. Instead you could simply subscribe to a monthly service and access the software using the maturing web browsing technology. There is a presumption that you would access the software over the Internet, which of course you can, however that's not to say it's the only way. The reasons behind this are plain to see, they did not want to limit their potential customers to those

being served by the network providers they were directly connected to. This is the real advantage of the Internet.

SaaS is still today the flavour of Cloud most familiar to us all. It does however carry with it both risks and limitations. The SaaS provider model says that you will share this software with many other individuals and businesses, can you be assured of privacy and confidentiality? There are also concerns around transmission availability and security if the if the software is accessed via the Internet.

Hosted Infrastructure

Hosted infrastructure is the next logical place that companies involved in building the Cloud will go. For those organisations that rejected the notion of SaaS because of its potential risks around privacy and confidentiality, but want to run their own software in a more dedicated and traditional way, outsourcing the infrastructure that runs their software was the obvious choice.

This type of Cloud is in-truth the oldest of them all, with mainframe computing being made available on a time-share basis from service providers as early as the late 1970's; it was not until the advent of x86 virtualisation by VMware in 1998 that the means to create a true utility model for IaaS was made possible. Whereas before VMware, hosting providers were forced to dedicate the hardware (even for a time) to each customer, VMware's virtualisation technology meant that IaaS providers could use a pool of hardware to provide per-customer dedicated infrastructure with the security and privacy assured via software separation.

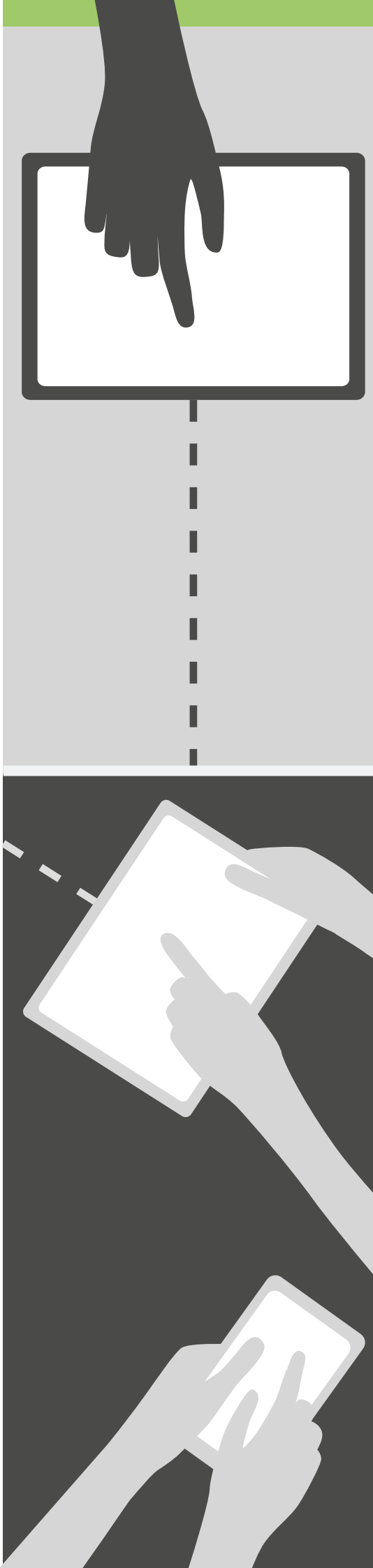
Today IaaS comes in many flavours from providers around the world; however not all IaaS is equal! There are, firstly performance concerns as the users often do not know how contended the underlying physical resources are and their computing workloads can often be left queueing. The quality and performance of the underlying hardware also varies greatly, and not uniformly with some providers offering fast processing but slow storage, others with powerful storage but dated processors, and very few with the latest and best of all types of hardware.

Secondly there is the question of access. While some potential gains in privacy and confidentiality can be realised by moving from SaaS to IaaS; the issues around transmission availability and security remain if the IaaS is accessed via the Internet. The separation between the servers, the data and those desktops and users working with it can also create tremendous issues in performance; and the desktop itself can often remain an unresolved security risk.

Hosted Desktops

The newest type of utility computing service to emerge is the hosted virtual desktop. This is an attempt to reunite the desktop and user interactions with the servers and data that had been moved to IaaS providers. Previously the limitations in access network speed and reliability, as well as issues with virtualising the graphical processing capabilities needed for modern computing posed a real challenge; initiatives such as the U.K.'s Super-Fast Broadband push and new technology from VMware together with graphics companies such as NVidia have made DaaS a reality.

Just as with IaaS, where software isolation provided a secure and private computing layer for users to run their software and store their data; DaaS provides the same capabilities to the client computing layer. This means each user has access to a virtual PC and these virtual machines will be either temporary, shared or persistent and dedicated just as IT departments would have provisioned on traditional desk-tied PC hardware. This means that IT departments can free themselves of the need to maintain any physical devices, and work entirely in a software-defined workplace.



Bring-Your-Own-Devices

The latter half of the 2000's saw the consumer leap-frog ahead of corporate IT, with the unforeseen demand for users to be able to bring their own IT devices into the workplace. Whereas before, computers and phones would be customarily issued as tools required for the job; now employees often have better computers and newer more powerful phones at home and questioned why they should be "downgraded" by their corporate IT department.

Many IT managers protested the loss of control and objected every step of the way, as they failed to see the advantage to users, who were already comfortable and familiar with the use and management of their own devices. A device which was already supported independently of the business helpdesk, and most importantly, a device which was already paid-for and would not impact on the budget of the corporate IT department.

Their concerns around allowing unmanaged and potentially insecure devices access to critical company infrastructure were however well founded. Fortunately the combination of DaaS, IaaS and SaaS which allows businesses to today create a software-defined workplace means that it is not only possible, but simple to allow these devices to access the company infrastructure in a safe and controlled fashion.

The key lies in creating a controlled and monitored environment where BYO and indeed any device can access the important gateways to the Internet and the virtual workplace without actually exposing any of the more sensitive software and none of the data stores. Users then login to their virtual workplace and receive not data access, but desktop access. In this way all data is stored within the Cloud, so there is no risk of the data being downloaded transferred or otherwise moved. The local device then becomes akin to the dumb-terminals of old but with a visually appealing interface and the design and use features most preferred by the individual user.

In the same vain as businesses today would rarely, if ever, consider an on premise safe as the best place to store their money but instead prefer a specialist institution that makes it their business to safely store, track and protect money; the Cloud represents the same model for storing data. Keep the data only in those premises and with those organisations that specialise in its proper care and protection. Allow only controlled and limited access to that data and move it from place to place as little as possible.

Legal & Regulatory Implications

When considering the move to the Cloud, the biggest differentiator from other utility industries is the nature of what data is. Whereas electricity, gas and water are all simple commodities, data has complexities we are only just beginning to understand. There is a raging debate in the courts of the world as to the questions of data ownership, be that its subject (the person who collected it) or its object (the person it regards). I do not think anyone today can predict the date we will achieve a global consensus on the correct and legal handling of data and so we must look at the world as a whole and consider carefully how it applies to us.

The legal sector in particular must consider the question of the controls around personal data (that data which is specifically about an individual). There are varying levels of control around personal data in play in the world today. Figure 1 shows a colour coded map highlighting the wide differences in personal data protection legislation from country to country. While technology developed in a less regulated country may deliver a boom in productivity, its use maybe completely illegal in another country with more stringent data protection regulations. It is therefore appropriate, especially for the legal sector, to consider carefully in which country they operate and work and where their data is domiciled and ensure their technology providers are familiar with the country's laws and regulations.

It may also be interesting to consider how these differing national attitudes towards personal information privacy can impact the interaction with clients. Around the world there is a general drive towards greater transparency. Perhaps the opportunity lies in giving the clients a more direct access and control to their own case files and legal folio via the same type of Cloud-driven virtual desktop?

Data Jurisdiction Considerations

The next pressing concern for the legal industry and perhaps the one which is not receiving sufficient thought today is that of data jurisdiction. Whereas in the past, we were only concerned with the physical location of the individual when it came to the application of the law; and we've since pressed forward with various rights of transference and extradition; we now must consider all these things anew in respect of the data.

Is data to be judged by the location of its user, its owner (knowing that

we are not even on solid footing in regards to determining the owner), or in-fact will decisions be made based on the location of the data itself?

In truth, data does not really exist anywhere, but we can make a convincing argument for the location of its primary non-volatile storage location. This location is often thought of as being the computer storage system, which is believed to store the most authoritative and permanent copy. While perhaps an oversimplification of the true problem, looking only at the physical location of the storage system is convenient and so is more often than not being called into scope of the law.

Historically it was sufficient for the data to not be somewhere in order to avoid a particular set of unfriendly laws; we now must consider that if (when?) we are brought to court, which court would we want to be in? An argument can be made then for literally jurisdiction shopping when it comes to our Cloud service providers (or at least those which house our most important data).

Is it safe, or advisable to store data with a provider who may replicate copy and archive or move the data between jurisdictions without explicit controls of the customer? As we can see in Figure 2 there is a horrendously complex latticework of legislation and international agreements that impact our data. All these concerns must be accounted for when moving to the Cloud.

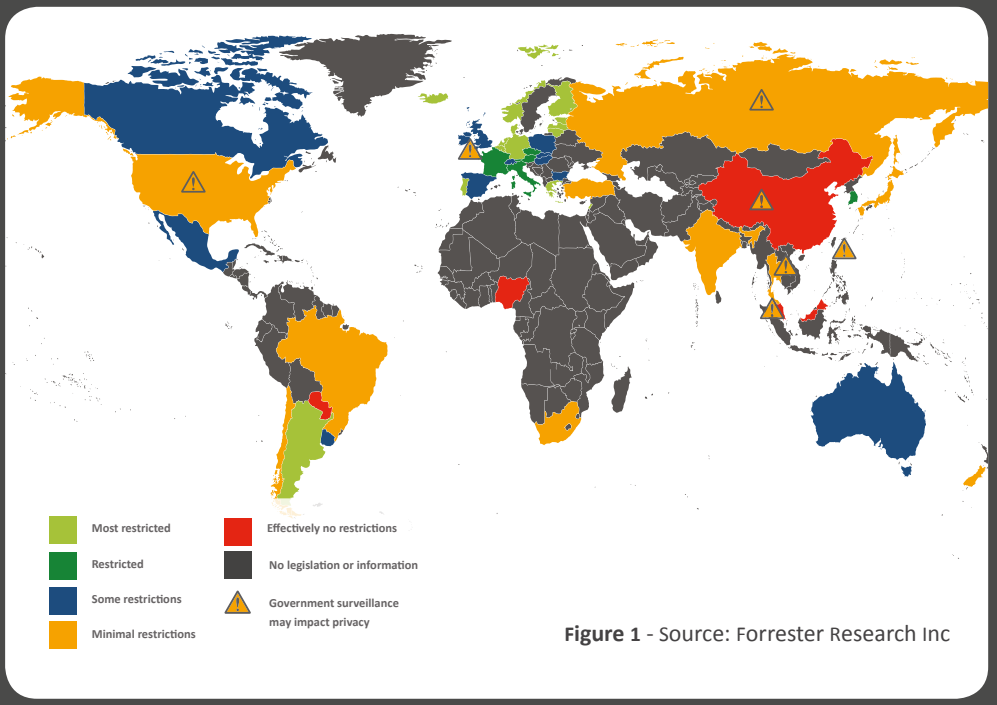


Figure 1 - Source: Forrester Research Inc

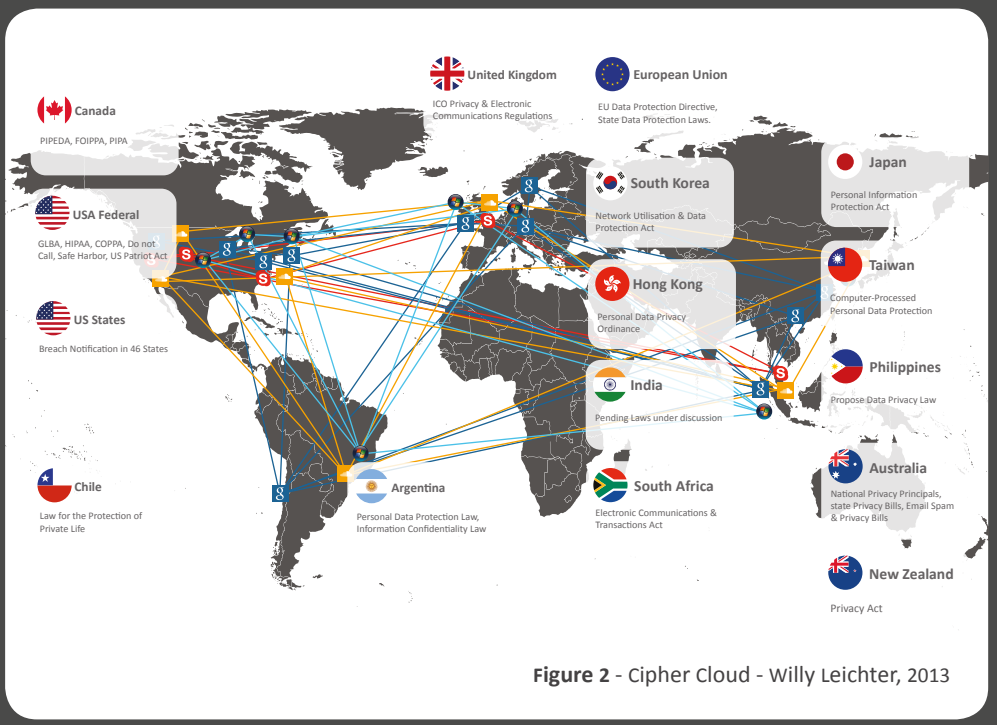


Figure 2 - Cipher Cloud - Willy Leichter, 2013

Electronic Signature Law

Finally for the legal industry to truly take advantage of the Cloud and this ability to move to a more, outsourced It model there is the question of the validity of the electronic signature. If we consider the future possibility where paper records are deemed less secure than electronic ones (as we've already seen with currency) it's important that the electronic documents can be appropriately signed.

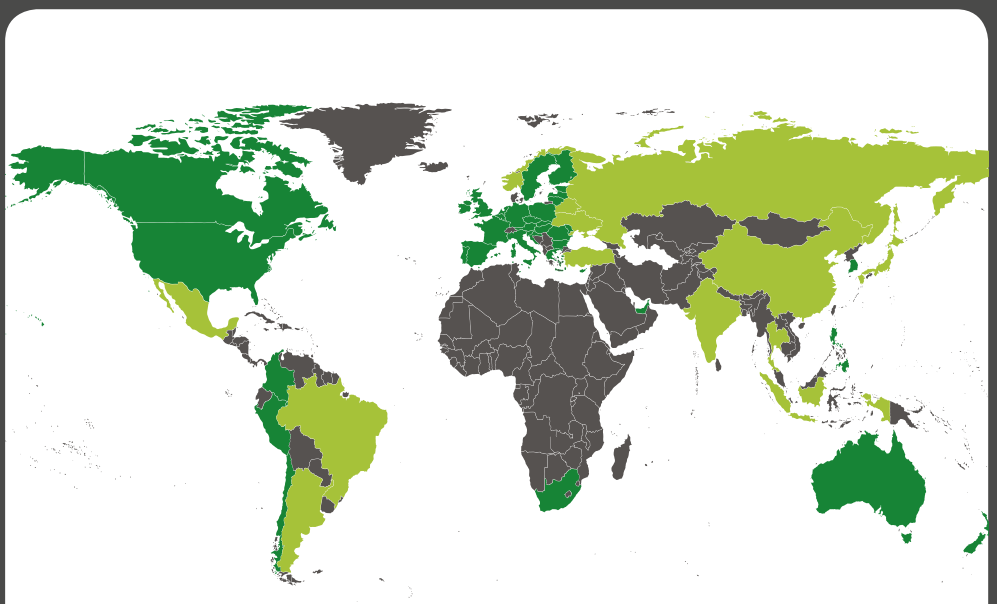


Figure 3 - Panadoc, 2014

Specialist companies such as Panadoc, have already developed the technology for the legal industry to take full advantage of electronic signatures in those countries where it is accepted.

In Figure 3 the dark green area represents those countries with full acceptance of electronic signatures today, the paler the shades of green indicates those countries with at least some acceptance. As we can see however there are other large parts of the world still in grey. For the legal industry to complete their move to the Cloud, lobbying needs to be done in these other countries to support the transition to electronic documents.

Privacy, Confidentiality & Security

No doubt the most challenging aspect of moving to the Cloud is that of ensuring privacy, confidentiality and security. In this area it is wise to look even closer at the finance industry and its handling of currency and other financial instruments. It should be obvious to accept that the best place to store anything important (data or currency) is with a business that specialises in its proper care and management. That simple fact aside however, one can see by observing the finance industry and its wealth of different accounts, products and services that there is no one-size solution. If we accept that data is significantly more complex than currency, there's even more expectation that any business will likely need a range of solutions working harmoniously together to achieve high levels of privacy, confidentiality and security.

Public Cloud

If we define public Clouds as those which service a wide range of customers on a single shared platform; accessible via the Internet we can then consider its correct application. The question to be asked is what (in particular to the legal industry) should be placed in a public Cloud. Ultimately the strength of the public Cloud, and indeed its very creation surrounds the serving of content and services to the general public over the web. There are no doubt a large number of legal applications for this in the way of automated law libraries, expert systems offering automated and autonomous advice and the like are perfect for this type of distribution model.

The inverse of this of course is that a publicly accessible model is not ideal for anything that requires higher levels of confidentiality and privacy. It's the Cloud equivalent of the difference between a daily-account with a debit card that can withdraw funds from the public high-street and a private banking facility that requires in-person interaction in private.

Private Cloud

Following the definition of Public Cloud, Private Cloud is the model where the Cloud service is more isolated per-customer, and connected privately to the customers internal network and not accessible via the Internet (other than by other remote access facilities). This makes Private Cloud an almost mirror image from Public Cloud where the users (consumers) of the data and services must first be inside the corporate domain before they are able to touch the Private Cloud services. This means it's not at all suitable for serving public facing information, but ideal for more confidential and mission critical systems and data.

Hybrid Cloud

As previously highlighted, all organisations will ultimately need a combination of different Cloud services which is exactly what Hybrid Cloud is. The key seems to be for most customers that this hybrid environment is only really a single environment when it's been well integrated into the secure private IT environment, which meets all the regulatory standards and business objectives.

Solutions

Highlighting the fact that the Internet is not synonymous with the Cloud, the real solution must begin there. The legal industry needs to establish within itself the guidelines for the use of private networking when connecting Cloud resources with IT and also guidance towards the proper residency of the data systems for the varying types of client and confidential data.

Once the Internet and Internet-based technologies are used appropriately with Private Cloud services making up the balance there are tremendous cost savings and efficiency gains to be had by outsourcing these critical, but non-core aspects of the modern legal business.

Consider moving not only files, servers and data-storage but also the main desktop points of interaction to the Cloud, as this will ultimately mean less data transport and greater security, privacy and control.

Conclusion

Change is inevitable, and with change comes opportunity. In much the same way as we moved our currency from bags of physical gold coin to almost purely electronic accounts managed by specialised providers we will evolve the handling of our critical legal data.

> ***"The traditional way of lawyering as we know it will go to the wall, without a doubt, but that's not to say there won't be new roles, new skills, new opportunities."***
>
> Lightfoot 2014

Awareness of the evolving nature of law and regulation surrounding information privacy, data residency and electronic signatures is key to successfully navigating the plethora of Cloud offerings in the market and determining their suitability and use in the legal industry.

By cost-optimising and right-sizing IT environments through the use of utility computing, both funds and mental energy can be directed more appropriately towards serving clients.

Secure but flexible virtual environments can act as virtual workplaces, where partner - client interaction and increased transparency is made easier without the restrictions of a physical location.

Online, massively distributed automated systems can provide anonymous advice and free service freeing partners to focus on fee-paying work while improving the public image and catchment of the firm.

Bring-your-own-Device can reduce workplace IT related stress, create a more self-sufficient and engaged user whilst reducing costs and complexity.

By restricting the copying, transport and location of electronic data and by eliminating on premise physical copies (including paper hard copies) we can greatly improve the security and privacy in the legal industry.
The Cloud model of IT is the answer to these and so many more challenges facing the legal industry today and it should be viewed as a positive change and on-going evolution of the great traditions and service of the legal industry, it should be viewed not as a threat, but an opportunity!

How Exponential-e can help you?

Professional Services:

Our highly qualified and experienced Professional Services team at Exponential-e will examine your existing infrastructure, consider your business' future needs and mitigate any risks to ensure a successful transition from Windows Server 2003. These practitioners are multi-skilled and uniquely placed to drive your business to an IT environment that will enable growth, flexibility, mobility of data, added security and compliance.

www.**exponential-e**.com/professional-services

IT Audit:

Avoid the headache of manually reviewing your IT estate with our IT Audit solution. Monitor all activity across your infrastructure with our single reporting tool, allowing you to see minute detail on things such as software installations and the utilisation statistics for individual users. The performance of individual machines will also not be affected due to the non-intrusive nature of the install.

www.**exponential-e**.com/it-audit

exponential-e
APPLIED INNOVATION

Works Cited: **Cipher Cloud** - Willy Leichter. (2013). "The Cloud Is Inevitable" - CipherCloud's Observations From Infosecurity 2013 In London. Retrieved from Cipher Cloud: http://www.cipherCloud.com/2013/05/10/the-Cloud-is-inevitable-observations-from-infosecurity-2013-in-london/ • **Lightfoot**, C. (2014) • **Tomorrow's Naked Lawyer**. ISBN: 978-1-78358-174-0 . • **Panadoc**. (2014). Where are electronic signatures accepted by law? Retrieved from Panadoc.com: https://www.pandadoc.com/electronic-signature-legality/