

CRITICAL DEFENCE

Life in the Cloud

Written By Mark D. Rasch, Vice President and General Counsel Critical Defence
January 2010

Is **Cloud Computing** really the next big thing? From a technological perspective it is hard to say. There are distinct advantages to being able to “lease” storage, processing, communications, platform, software and other infrastructure, and to be able to access information from a variety of platforms anywhere in the world. From a legal perspective however, cloud computing is another in a series of next big things that changes everything. Just as the Internet itself modified such traditional legal concepts as trespass, and jurisdiction, and social media sites inextricably changed legal concepts like defamation and publication, cloud computing continues this trend by challenging notions of ownership, physicality, possession, custody, control, sovereignty, and even consent. If the Internet generally is to the law as “new wine” is to “old bottles,” cloud computing is both new wine and new bottles.

This matters because the law traditionally deals with new situations by attempting to refer to old situations for which there is an established legal regime. Thus, a “trespass” to a computer is analogized to a “trespass” to a bedroom – entering or remaining in a place without appropriate authorization. However, these analogies break down quickly, and there is a gap inevitably left in the law.

How Cloud Computing Changes the Law

If you ask a dozen IT professionals what cloud computing is you are likely to get more than a dozen answers. In its “purest” form, all digital information and processing is transferred to an amorphous online environment – the cloud. You don’t create documents on a laptop computer using a software program. Rather you access an online word processing or spreadsheet program and create and store the ensuing document in the cloud. You don’t own the software that you use to create the program (well, actually you don’t technically own it now – you pay for a software license – an authorization to use it). In the cloud, however there is no tangible “thing” to own – no CD-ROM or DVD. Because the software resides on the cloud, it is always up to date, and can – and the emphasis here is on “can” – be made to be reasonably secure. Instead of an enterprise with 1,000 copies of Microsoft Word of all different flavors, versions, sub-versions, settings and configurations running on a half dozen different platforms, everyone in the enterprise logs in and has instant access to the most up-to-date version of the software which has presumably been patched by the “cloud owner.”

Software Ownership

Just this simple application of the cloud has a fundamental impact on things like copyright law, software licensing, and user expectations. While many such “cloud” applications (like Google Documents or Google Spreadsheets) offer an open source license, more traditional software providers are likely to charge some kind of licensing fee for the ability to use their online software. This could be a subscription type service – for a few bucks a month, you get the ability to use the latest and greatest version of the software. But if you fail to pay or if the

provider fails to acknowledge your payment, the software dies, and with it your ability to effectively access your documents.

In the early 1980's, software developers would put secret logic bombs into their software, which would automatically "kill" the software if the developer failed to input a code. If the software lessee (the customer) failed to pay, or if the developer felt that the contract was in some way breached, the developer would just fail to input the appropriate code and "poof" the software was disabled, and the business shut down. At the time, several courts held that this constituted unlawful "self-help" in a contract dispute, or alternatively a form of extortion, but they relied on the fact that the existence of these logic bombs was not disclosed to the customer.

In the world of the cloud, software license disputes could result in the effective remote termination of access to critical software. Is this extortion? Is it legal? Ultimately it will depend upon what is disclosed in the software license agreement (SLA) between the cloud provider and the customer – and the willingness or ability of the customer to read and effectively negotiate the contract.

Thus, while Microsoft's "Genuine Advantage" code has the ability to prevent software it believes is unlicensed from either working, working efficiently, or receiving essential updates, a user willing or able to work completely offline may be able to thwart the anti-piracy code. The nature of the cloud means that these pirates (and sometimes their victims) can be remotely killed – sometimes with little recourse.

Data Ownership

The Internet has made a mess of the concept of data ownership, and the cloud not only continues but exacerbates this problem. The phone company for example has records that relate to my bill – who I called, when I called them, how long I spoke with them, etc. They also have the contents of every text or SMS message I may have sent or received. As an ISP, they have the contents of every web browsing session from my mobile phone, and every e-mail sent or accessed via the phone. They also know the GPS (or rough GPS) coordinates of everywhere I (or my phone) have been, how fast I was driving, and through data mining of others' records, who I was with.

While some of these records are afforded legal protection against unauthorized disclosure of use by statute, much of it is in a murky legal netherworld. For example, the records of my use of the phone (billing type records) belong to the phone company. The contents of my emails and conversations "belong" to both of us, but there are laws prohibiting the phone company from disclosing them without proper legal process. The GPS data can be interpreted as just technical engineering information about signal strength or the like (so the phone company owns it) or intimate personal information about a consumer.

Irrespective of who "owns" the phone company data, there is a related issue of who "possesses" it. As a result, even if my e-mails are my "property" the phone company, which is in possession of them, can be forced to turn them over, say in the event of a subpoena, demand letter, or court order.

In the cloud, it is possible that ALL digital information will reside in the ether. Not only my calendar, phone calls, contacts, and friends, but every document, diary entry, magazine article, video chat – everything. My documents will no longer be on my desktop or laptop, or on my corporate server, but they will be on some cloud provider's server or servers in any nation in the world.

Just as a litigant (say the government) who wants my e-mails may, with appropriate legal process, bypass me and get my mail from my ISP or phone calls from the phone company, a litigant in the cloud can bypass my company's counsel and get all of my documents from the cloud provider. Indeed, I may or may not ever know that it happened. While it is standard to put into an agreement language mandating that data be protected and not disclosed, the same standard language also indicates that the data holder (not the owner) will, of course, be bound to comply with subpoenas and court orders.

Thus, cloud computing – and the concept of living life on the cloud – fundamentally changes notions of ownership of data, access to data, possession of data and the like, and replaces it with related concepts like “right to privacy in data” or “expectations of use” of data. Why is it that when you send an e-mail you accept the fact that the ISP may be forced to reveal its contents with just a subpoena (and not a search warrant) but you would never expect your landlord to be forced to give up the contents of your bedroom without a search warrant? It is because you feel territorial over your apartment (it's YOURS) but not over your electronic data (well, nobody could expect that to be private.)

As a result, a document may have different privacy expectations if it is on a laptop in your apartment, on an e-mail server, or in the cloud. Even if the ownership of the document remains the same, the fact that the document can be accessed remotely and is stored by a third party affects its privacy and security.

Sovereignty

If you live in the United States you are entitled to certain rights by virtue of your residence and/or citizenship. The same is true of France, the Netherlands, Japan or any other nation. Each country has the authority to regulate the conduct of its citizens (in law called the citizenship principle); of things that occur within its borders (the territorial principle) ; or things that may affect things within its borders (territorial protective principle.) Each nation has its own laws, customs, values and procedures that it imposes on those within its control. Some cultures and legal systems respect privacy more than others, some respect authority, some individuality. Thus, issues like distribution of pornography, online gambling, or political speech may be treated very differently by different cultures.

The speed and reach of the Internet has already transformed the way countries deal with activities that occur remotely but impact a national interest. A fraud scheme in Nigeria can immediately have an impact in New York. Gambling in an online site in Monaco may actually be occurring in Montana. Issues of choice of law, sovereignty, venue and jurisdiction already are pervasive on the web.

The cloud makes these problems even worse. A company doing business in Nebraska may find its critical documents located on a server in Namibia. Nation-states tend to think that they have jurisdiction over physical objects or things within their territorial boundaries. Thus, while it makes no difference to the cloud where a server or records are located, it makes a difference to the country. Information that is protected from disclosure in one country may not be afforded that protection when the same information is physically located in another country. The cloud permits documents to be in many countries at the same time. Moreover, companies or individual that have no meaningful business contacts in a country (and therefore no reason to be concerned about the law of that country) may find themselves subject to some foreign law (whether it be federal, state or municipal law) because their data has migrated into that country. Similarly, trans-border data privacy laws limit the authority of entities that collect personal information about residents of one nation from transferring that data to another country that does not afford that data at least a similar level of legal

protection. If a U.S. company collects and stores personal information about a German citizen, it must comply with the laws and directives of the German Data Privacy Commission. Before the U.S. company can transfer this data to a server in the United States, it must provide assurance that the data will be both physically and legally protected from unauthorized disclosure. Enter the cloud. The data is now collected about a German citizen by a U.S. company, with all of the requisite assurances, but now it is stored on a cloud platform. Thus, the data now “resides” not in the United States, but say, in the Philippines, or Fiji, or Tasmania. Does Tasmanian law protect the privacy of German personal information? Can the Tasmanian government legally seize and examine the information on the server? The law truly gets clouded by the new technology.

Audit and Assurance

In the classic computing model, a company stores data on its servers, and protects that data with layers of security at the data, application, transport, storage, network and access levels, among others. Imagine an office within a larger office building, within an office park in a neighborhood. If you lease office space, you can protect data by your “ownership” of the filing cabinets and desks (which you can lock), and your authority to lock the front doors of your particular office or set of offices. This is primarily your responsibility. You may also have a receptionist to control access to your office or office suite. The security of the office building lies generally with the building owner or manager, and is set by some sort of agreement between you and the owner. The owner will provide a security guard or guards 24/7, will require some form of ID for entry, will have a badge access system for the elevators, will patrol the building for unauthorized activities, and will call the police if anything suspicious happens. The owner of the office park itself (if different from the building owner) may add private security patrols, security cameras, etc. All of this is set out in an agreement between the parties.

Similar situations occur within the cloud. While you may own the data, the “file cabinets” “offices” and the entire infrastructure is, in effect leased from the cloud provider. What is not settled is who has the duty, authority and responsibility to protect that infrastructure. Typically this will be done through an agreement between the parties – a Service Level Agreement or SLA. In the office situation, much of the security and access control “agreements” are not contained in the lease. They are implied. Nowhere in the commercial lease for example does it say that the security guard will call 911 if they see an office being burglarized. The level of security, training and awareness are not specified in the lease. Nor are things like the thickness of the walls, the spacing of the security cameras, the resolution of the cameras, etc., unless there is a specific security need (e.g., a Secure Classified Information Facility or SCIF, or a particularly secured location.)

The cloud typically would contain routine “every-day” communications, as well as the company’s most important family jewels. Who is responsible for data classification in the cloud? Who is responsible for data-level security? What are the levels of protection and response? Since no assumptions can be made, all of this should be specified in the SLA. However, as technology advances, new services offered, and the cloud expands, the SLA will quickly become outdated. It is also difficult to anticipate the level of need for security at the outset, and no SLA can anticipate every potential problem. There is not yet an agreed upon set of security standards for cloud providers to provide not only for storage, but for transmission, processing, applications, etc. Finally, there is the problem of audit and assessment. Who has the legal obligation to assess the level of security provided by the cloud provider? If you were putting your critical data into a U-Haul storage facility, you would not expect to be required to conduct a daily or monthly assessment of the security – that

would be the responsibility of the storage facility, right? But when your critical data is stored or processed in the cloud, you would want to know how it is being protected. Should the cloud provider simply give some written assurance of security, like “we comply with the requirements of GLBA, SOX, or ISO standards?” Who pays for the audits? Can the cloud customer see the results of the audit? If the answer is yes, and the audit shows vulnerabilities, doesn’t the cloud customer now know how to exploit OTHER cloud customers on the same cloud? Not so simple. In addition, many of the legal requirements for privacy and security are essentially non-transferrable. As a data collector, you have a responsibility to ensure that the information is secure. “My dog ate my homework” won’t work anymore than “my cloud ate my data.” All of these problems are exacerbated in the cloud.

It has been said that every cloud has a silver lining. With all of the rewards that cloud computing offers, it is important to remember that every silver lining also has a cloud – and sometimes that cloud is in the form of a lawsuit. Just remember that I’ve looked at clouds from both sides now, from good and bad, and still, somehow, I really don’t know clouds – at all.

Mark D. Rasch is a former U.S. Department of Justice Prosecutor that specializes in Computer Crime and Electronic Incident Response. Mark currently serves as the Vice President and General Counsel of Critical Defence LLC. Critical Defence provides strategic risk consulting solutions that enable public and private sector clients to effectively plan for and respond to the latest security threats.

Have a question? Mr. Rasch may be contacted by email at mrasch@criticaldefence.com.