# Cloud Computing Customers’ “Bill of Rights”

***By David Navetta***

*During the course of our firm’s work with clients, especially on the customer side, certain “roadblocks” consistently appear which make it very difficult for organizations to analyze and understand the legal risks associated with cloud computing. In some instances this can result in a willing customer walking away from a deal. So we thought it would be a good idea to create a very basic “Bill of Rights” to serve as the foundation of a cloud relationship, allow for more*

*transparency and enable a better understanding of potential legal risks associated with the cloud.*

*While we use the strong term “rights,” we know that cloud arrangements vary and that every transaction has its own issues and circumstances that impact the nature and scope* of a negotiation. Moreover, as with the real Bill of Rights, we realize that none of these rights are absolute and may appropriately be subject to reasonable limitations in certain contexts. This article should be viewed less as a universal mandate, and more as a tool for cloud customers and providers to engage in spirited debate about the issues addressed in this new cloud computing Bill of Rights.

# Cloud Customers' Bill of Rights (Annotated) Article I – Data Location Transparency

*Cloud service providers shall reveal the physical location of the servers that will be processing their*

*cloud customers’ data, and shall provide reasonable advance notice if those physical locations change; cloud service providers shall coordinate with their customers to assure compliance with local laws and any applicable restrictions on the transfer of certain categories of data from one jurisdiction to another.*

**Comments:** The bottom line for this right is that in this day and age, for better or worse, the nature of the data and the physical location of its processing dictate legal obligations of cloud customers.

Transborder data flow issues are not new, but they are magnified in the cloud context where the free flow of data across borders may be the norm (and this free flow will only increase as the “Intercloud”1 arises and data processing begins to behave more like electricity).

The classic example is the EU Data Protection Directive.2 A company that moves data made up of personal information of EU residents outside of the EU to certain countries (like the U.S.) risks a violation of EU law. In addition, the recent privacy law3 passed by the Canadian province of Alberta prohibits the transfer of Canadian personal information outside of Canada without providing certain

1 <http://www.helium.com/items/1967022-cloud-computing>

2 [http://en.wikipedia.org/wiki/Data\_Protection\_Directive.](http://en.wikipedia.org/wiki/Data_Protection_Directive)

3 <http://www.infolawgroup.com/2010/05/articles/breach-notice/faq-on-albertas-new-breach-notice-law/>



**PAGE 3**

**INFORMATION SECURITY & PRIVACY NEWS**

notices to the data subject. Another example is the desire for some entities4 to avoid having their data processed on U.S. soil because of the USA Patriot Act. The processing of data in an unexpected country might also generally implicate jurisdictional issues5 over a particular cloud customer. Finally, in another twist, having to disclose certain data that is subject to a discovery request could run afoul of privacy laws in certain jurisdictions6 -- forcing the cloud customer to choose between violating the law and losing their lawsuit if they don't produce the evidence.

Cloud service providers that fail or refuse to reveal where their customers’ data is being processed risk exposing their customers to significant regulatory and legal risk. Unfortunately there are some

providers that simply to refuse to provide this information (either because they don’t want to, or

perhaps because they don’t know or can’t keep track of where data is being processed). Other cloud providers are more sensitive to this issue and will actually contractually agree that their customers’ data will be processed only in certain countries or locations. Nonetheless, for cloud customers to truly understand the legal risk of the Cloud, they need this information.

# Article II -- Security Transparency

*Cloud service providers shall provide full information and access to documentation concerning their security policies and measures, including the ability for cloud customers to conduct periodic security assessments and obtain relevant security-related information and documents from the service provider; this information and documentation should address data integrity and availability as well as the confidentiality of customer data.*

**Comments:** Cloud customers may be ultimately liable for security breaches suffered by their cloud service providers. Moreover, cloud customers may have legal obligations to maintain certain security measures. These obligations do not disappear just because a customer’s data is being processed by a cloud service provider. Yet, in many cloud transactions, getting good information about security can be very difficult. While many cloud service providers are willing to provide SAS70 reports, if not tied to established data security standards such as ISO 27002,7 these reports may provide only a limited picture of security (and often the picture limited to that which the provider desires to reveal). Unless the cloud customer is a large entity (and even then), most cloud providers will not allow for an independent security assessment by the customer. Moreover, in long term relationships, a cloud

provider’s security stance may change. Even if in-depth information is provided at the outset of a cloud relationship, if security is not allowed to be revisited, cloud customers may be at risk. Similar to the data location issue, this can result in very unpleasant surprises in the form of security breaches,

4 <http://www.enterprisestorageforum.com/outsourcing/article.php/3904981/Could-Borders-Bring-the-Cloud-Down-to-> Earth.htm

5 <http://www.glgroup.com/News/Who-has-Legal-Jurisdiction-in-the-Cloud--50084.html>

6 <http://www.law.georgetown.edu/cleblog/post.cfm/district-court-orders-production-despite-german-data-protection-act>

7 <http://en.wikipedia.org/wiki/ISO/IEC_27002>



**PAGE 4**

**INFORMATION SECURITY & PRIVACY NEWS**

lawsuits and regulatory actions. As such, from the cloud customer point of view, transparency around a cloud provider’s security is of paramount importance.

# Article III -- Subcontractor Transparency

*Cloud service providers shall provide cloud customers with notice as to which third parties will have the ability to access customer’s data and for what purposes, including subcontractors, subcontractors of subcontractors and so on.*

**Comments**: It is not an uncommon for cloud customers to discover that the cloud service provider with whom they are entering into an agreement is not the sole entity that will be processing their data. The classic example is a SaaS running on a third party cloud. These relationships may be more attenuated than meets the eye as there may be third and fourth levels of cloud providers processing customer data, and the cloud customer may have no idea who is actually handling their data. Even if a cloud provider has revealed its subcontractors at the outset, it is not unusual for a cloud provider to switch subcontractors in the middle of a contract term. From the cloud customer’s point of view it is important to know exactly who will have access to its data, and whether those entities pose additional risk. Unfortunately, these subcontracting relationships may not be revealed up front by cloud providers, and are even less likely to be revealed in the middle of a cloud relationship. Rather, many cloud contracts contain clauses that provide the service provider with the right to use third parties, or are silent on the issue. As such, some cloud customers may want to impose certain contract conditions to govern the use of subcontractors.

# Article IV -- Subcontractor Due Diligence and Contractual Obligations

*Cloud service providers shall conduct reasonable due diligence and security assessments of subcontractors or other third parties that will have access to customers’ data or systems, and shall enter into contracts with such third parties that hold those third parties to substantially similar obligations as in their cloud agreements with their customers; cloud service providers shall manage and similarly limit the ability of their subcontractors to utilize other subcontractors.*

**Comments:** As a corollary to Article III above, to the extent that cloud providers do utilize subcontractors to process their customers’ information, a proper vetting of those subcontractors is

appropriate, as well as certain contractual obligations. The providers’ due diligence should include not only data security and privacy assessments of their subcontractors, but also more generally ensuring that their subcontractors are capable of carrying out the promises made by the cloud providers to their customers. This due diligence should be buttressed by contractual obligations imposed on subcontractors that match those made by the cloud provider to its customers. Finally, both for their own protection and the protection of their customers, cloud providers need to worry about and limit their subcontractors’ ability to use subcontractors further down the line.



**PAGE 5**

**INFORMATION SECURITY & PRIVACY NEWS**

# Article V – Customer Data Ownership and Use Limited to Services

*Cloud customers shall have the right to solely “own” the data they put into a cloud service provider’s cloud, and cloud service providers shall use their customers’ information solely for the purposes of providing services to the customer, unless otherwise explicitly agreed.*

**Comments:** Certain types of data flowing through cloud providers’ systems is extremely valuable (e.g. personal information of users) and there may be some temptation to use or exploit this data (or perhaps it is part of their business plan). Customers will expect that their cloud providers acknowledge that the customers are the sole owners of that data relative to the providers, and that the data should only be used to provide services to the cloud customer. In fact, this was one of the key requirements8of the City of Los Angeles when it agreed to use Google cloud services. If service providers are going to use data beyond the purpose of providing services, prior notice to their customers should be provided. Service providers that do use their customers' data beyond primary purposes risk hurting their customers’ relationships with their clients and customers, and risk rendering their customers in violation of their privacy policies or data privacy laws.

# Article VI – Response to Legal Process

*Cloud service providers shall provide notice (within hours, not days) of the service of any subpoena or other legal process seeking their customers’ data, and shall assist and cooperate with their customers in responding to such legal process.*

**Comments:** The ability of a cloud customer to understand when the government is seeking their data is crucial for managing legal risk. If a cloud service provider sits on a subpoena or other legal process it could harm the target customer, and hamper its ability to adequately respond to such a request and develop legal positions. Cloud service providers should develop a process for promptly dealing with these requests and providing notice to their customers. In the cloud context, with data potentially distributed across multiple geographically distant data centers, developing an efficient process and information flow may be challenging.

# Article VII -- Data Retention and Access

*Cloud service providers shall reveal their data search, retention and destruction practices to their cloud customers; and shall develop and enable data search, retention and destruction capabilities in order to allow their customers to implement their own data retention programs, efficiently effectuate litigation holds, and locate, collect and preserve relevant data, including metadata; cloud service providers shall*

8 <http://www.infolawgroup.com/2010/05/articles/cloud-computing-1/whats-in-googles-saas-contract-with-the-city-of-los-> angeles-part-one/



**PAGE 6**

**INFORMATION SECURITY & PRIVACY NEWS**

*build in processes and controls that allow for the efficient authentication of data (e.g. accurate time- stamping; metadata; chain-of-custody indicators, etc.).*

**Comments**: Most sophisticated organizations have data retention policies and procedures in place for executing a litigation hold and preserving data. Implementing these policies and procedures internally can be a challenge, and that challenge is magnified significantly in a cloud environments where the customer must rely on a third party, the flow of data is very fluid, and data may be intertwined with the data of multiple cloud customers. In an environment where proper eDiscovery and electronic evidence practices can make or break a lawsuit, the search, retention and preservation capabilities of a cloud provider are very important. Cloud customers will be seeking to ensure their own internal

policies can be followed in their cloud provider’s environment. On the front end, this requires transparency and the availability of technologies that enable the efficient identification, collection and preservation of data. On the back-end, service providers will be expected to cooperate with and assist their customers with obtaining electronic evidence and responding to electronic discovery requests. As discussed with respect to Article VIII, this may be tricky in the cloud context, especially when it comes to a cloud customer's desire for an independent forensic investigation.

# Article VIII -- Incident Response

*In the event a cloud provider suffers a security breach, Cloud providers shall provide prompt notice of the security breach to their affected cloud customers, shall coordinate, cooperate and assist their customers with the investigation, containment and mitigation of the breach, and shall allow their cloud customers to conduct their own forensic assessment and investigation of the security breach.*

**Comments:** Similar to issues around litigation holds and data preservation, cooperation and coordination is crucial when a cloud service provider suffers a security breach. Again, it is the service provider’s customers whose business will suffer due to a breach, especially if procedures are not in place for the containment and mitigation of a breach. This again requires service providers to provide transparency as to their internal incident response processes so that cloud customers can ensure that their own internal incident response policies match up. Also of significance is the ability of cloud customers to access their service provider’s facilities and systems in order to conduct their own forensic security assessment. This is important not only for data preservation, but also for substantive defense issues. Cloud customers need to be able to conduct such assessments to determine what went wrong, whether any laws may have been violated, the defenses that may be available to the company, and who was responsible for the breach. On the latter question, in some cases it may be the service provider who was at fault, which makes getting access an interesting proposition. Moreover, the multi-tenancy nature of cloud computing also poses challenges. Some cloud providers claim that independent forensic assessment is not possible because it could expose the data of the provider’s other customers and potentially result in a violation of a non-disclosure agreement. Needless to say this is a very trick issue.



**PAGE 7**

**INFORMATION SECURITY & PRIVACY NEWS**

# Article IX – Indemnification and Limits of Liability

*Cloud service providers shall engage their customers in meaningful discussions and negotiations around indemnification and limitations of liability arising of security breaches, including consideration of exceptions to limits of liability for security breaches suffered by the cloud service providers.*

**Comments:** The reality on this “right” is that for “commoditized” cloud service arrangements there will often be no or very limited negotiation on terms (terms will often be reduced to clicking “I agree” on a website). However, in other cloud service transactions, where the parties are on more equal ground in terms of bargaining power, these terms are and should be up for negotiation and debate.

From the customer perspective, it is ceding control of some of its most precious assets: its ability to provide its goods or services, and its data. When a customer suffers a breach internally its incentives are to mitigate the breach and potential adverse consequences to the organization. In the cloud context the service provider’s interests may not be aligned with those goals (in fact, to the extent the service provider was at fault, its interests may run counter to its customers'). Service providers, may choose to put their own considerations very high up. Also to the extent a breach involves multiple cloud customers, cloud service providers may also favor the interest of particular customers over others. This lack of control and reliance on the providers justifies serious consideration of

indemnification clauses, consequential damages disclaimers and limitations of liabilities. In some cases, service providers may provide higher limits of liability (or even no limits of liability) for confidentiality breaches or security breaches.

*David J. Navetta is one of the founding partners of the Information Law Group. David focuses on technology, privacy, information security and intellectual property law. He is also a CIPP. David has enjoyed a wide variety of legal experiences that have provided him with a unique perspective and legal skill set, including work at a large international law firm, in-house experience at a multinational financial institution, and an entrepreneurial endeavor running his own law firm. Prior to co-founding his current firm, David established InfoSecCompliance LLC (“ISC”), a law firm focusing on information technology-related law. He previously worked for over three years as assistant general counsel and was engaged in commercial litigation for several years prior to going in-house, working at a large international law firm. David has spoken and written extensively about the legal risks and issues associated with cloud computing, including numerous publications on his firm’s site:* [http://www.infolawgroup.com](http://www.infolawgroup.com/). *He is also co-chair of the ABA’s Information Security committee.*