



Is SaaS Really Better For Business Than Software Licensing?

White Paper

August 1, 2007

Copyright James River Consulting LLC



James River Consulting

Better IT Contracting

www.jamesriverllc.com

134 Hillside Avenue, Needham, MA 02494 703.850.7061-Mobile
info@jamesriverllc.com jamesriverconsulting@comcast.net

Introduction

There is a prominent Software as a Service (SaaS) provider whose marketing campaign includes a red-circle-and-slash symbol over the word “Software” and a toll free number that reads “NO-SOFTWARE.” It’s a provocative ad that is emblematic of the IT industry’s new attitude towards selling software as a service instead of licensing it.

The Software and Information Industry Association, the preeminent software trade association, calls SaaS a “revolution” that addresses licensing’s runaway costs of ownership. The SIIA’s white paper entitled “Software as a Service: A Comprehensive Look at the Total Cost of Ownership of Software Applications,” cites a 2003 IDC head-to-head comparison of costs of ownership between software and SaaS. The IDC study shows a quickly leveling line for SaaS costs over a 3 year period, compared to a steadily ascending line for comparable software culminating in 174% higher costs for software by year 3.¹ Clearly there is potential for huge cost savings with SaaS.

The SIIA white paper also gives data on the proportionate cost of licensed, on premise systems compared to SaaS subscription costs. SIIA concludes that the initial investment in infrastructure for licensed systems including applications, hardware and training is as little as 5% of the total cost of ownership over several years, with

¹ Figure 9: IDC’s comparison between traditional software and SaaS, Software as a Service: A Comprehensive Look at the Total Cost of Ownership of Software Applications (September 2006, SIIA Executive Council on Software as a Service). The graphic is used to refute the premise that the upfront costs of licensed software reduce costs below those of SaaS in out years.

associated personnel costs accounting for as much as 85%.² For that same period, SaaS subscriptions account for 80-90% of all ownership costs.³ The difference in these percentages is another huge advantage for SaaS because it makes calculating return on investment (ROI) more predictable than doing so for software, and moreover SaaS’ service nature allows for continuous reassessment of ROI. ROI is licensed software’s in the B2B market mostly has been poor to none.⁴

An even more extreme version of SaaS being bandied around, called “utility computing,” promises to render computing into a metered utility just like water and natural gas. While pointing to a future computer utopia, at present the concept is limited to utilizing existing hardware assets more efficiently and the tracking application usage by internal users and data center customers.

In all likelihood the SaaS model will soon replace perpetual licenses as the predominant model by which software is bought and sold. Gartner predicted in October, 2006, that by 2011, 25 % of new business software will be delivered as SaaS.⁵ Triple Tree, a Minnesota investment bank and consulting firm, makes a more

² Figure 7: Summary of the cost allocations of a traditional software deployment, “Software as a Service: A Comprehensive Look .”

³ Figure 8: Summary of the cost allocations of a SaaS deployment, “Software as a Service: A Comprehensive Look.”

⁴ A James River Consulting will publish a white paper comparing performance measurement for SaaS, perpetual licenses and outsourcing in Fall, 2007.

⁵ “Gartner Says 25 Percent of New Business Software Will Be Delivered As Software As A Service by 2011” Press Release, October 3, 2006, Gartner, Inc.

aggressive (and more accurate) prediction, that 40% of all software will be SaaS by 2009.⁶ The caveat to this trend will be enterprise wide, “mission critical” or “core” software systems, which require greater customization and integration than is currently contemplated by the SaaS business model. Encompassing enterprise core apps is unlikely to happen going forward. From a vendor standpoint, the practice of trying to customize an application on a customer-by-customer basis is blamed in part for the early demise of the application service provider (ASP) software model in the early 2000’s. From a customer standpoint, recent news articles on SaaS implementations of enterprise systems by corporate customers confirm the infeasibility of SaaS for these systems.⁷

But what are the overall risks and rewards with SaaS for business customers and do they leave customers better or worse off than they are licensing software and implementing on premise systems? Cost is only one piece of the puzzle. This white paper will focus on SaaS risks and rewards as compared to those of the traditional perpetual software license from a contract rights and liabilities perspective.

Licenses versus Access

We begin the comparison by looking at licensing itself as a method of transacting. Software is a licensed commodity because, after much debate in the 1970’s and early 80’s in both the courts and Congress, it was decided software contains intellectual

property rights (later in the 1990’s software was deemed to contain patent rights as well). At issue was copyright’s original purpose of protecting artistic works. Computer code operated machines, you did not read it or listen to it. Licensing has never been a perfect way of selling software for either buyers or manufacturers. When you buy a book or a CD, you buy it subject to an unseen license in the form of copyright laws. You are free to sell the book or CD and the license automatically goes along. Software comes with a written license that spells out your rights, not only the copyrights, but other rights as well since software is interactive and more complex. Unlike a book or a music CD, you are not free to sell the software because it is only licensed to you. Further, the software code itself can be taken away from you if you violate the license terms.

Over the years software licenses have evolved into fairly lengthy documents containing a multitude of provisions that are far removed from the intellectual property rights. Support agreements and auditing methods are two examples. Regardless, once a user has violated any term in the license document, all right to use the software is lost for ever.

The single biggest inequity of licensing as a method of selling software is and has always been the potential permanent loss of user rights, and total loss of any initial software infrastructure investment without chance of refund, for even minor technical violations. The only method of redressing the problem is to negotiate the software vendor’s boilerplate agreement, a near impossible task for all except the largest corporate buyers. In practice, software vendors mostly

⁶ Software as a Service Update Report, September, 2006, Triple Tree LLC.

⁷ G. Gruman, The Truth About Software as a Service (SaaS), CIO Magazine, May 21, 2007.

use license violations to leverage selling more software, not to terminate which would alienate customers and incur legal fees.

Bottom line, the licensing model motivates software vendors to write licenses with more and more restrictive terms as a tool for increasing revenue. In the late 1990's some software OEMs tried to take this onerous characteristic further by supporting a "self help" provision in the Uniform Computer Information Transactions Act (UCITA) which legalized remotely disabling software for license violations. After a groundswell of opposition from consumer rights groups like Americans For Fair Electronic Transactions (AFFECT), the self help idea was dropped and UCITA was eventually abandoned.⁸

Conceptually, SaaS is a service, more specifically a software access service. Unlike licenses, with SaaS there is no delivery of an actual copy of software code or installation of a copy of code. Besides access, passwords and online or telephone support are the only other essential deliverables. With licenses, a formal transfer of intellectual property rights takes place. But with SaaS, there is no, or at least minimal, licensing of intellectual property.⁹ Property rights are regarded as assumed into the service. Unauthorized access (if there is such a thing, depending on how the SaaS serviced is defined) becomes the chief and

⁸ Section 602, Uniform Computer Information Transactions Act, Amended 2002, National Conference of Commissioners on Uniform State Laws.

⁹ A discussion of the transfer of intellectual property rights in a SaaS service is outside the scope of this white paper.

only concern of the provider, not unauthorized copying to avoid license fees or reverse engineering in order to build a competing product.

Hence, SaaS should present far less risk for customers than perpetual licenses. By reducing software transactions down to simple access and payment, the SaaS model should reduce the risk of total loss of use and loss of initial investment to nil, and SaaS customer should have no worries that they will somehow violate contractual terms. Further, customers should avoid the risk of agreeing to restrictions on rights of use in licenses that they must subsequently remedy by buying more licenses. Instead of the lengthy license agreements and myriad of legal provisions that have become the norm in the B2B software market, SaaS should make the legal aspects of software transactions cut and dry.

SaaS Service Agreement Terms

A number of current, prominent SaaS providers make their service terms and conditions available on their Web sites. A random survey of these online documents by James River Consulting over a period of several days, from July 20-25, 2007, shows that SaaS providers have not exploited the simpler and less risky nature of selling software as a service. In fact, in ways that are explored below, current SaaS terms and conditions present a greater risk of loss of user rights and fees than licenses. In addition, current SaaS agreements introduce new and significant risks for customers not present with licensing.

For discussion purposes, we will compare licenses to an online SaaS services agreement for a fictitious SaaS provider

named Sellhard.com. The terms of Sellhard.com's agreement represent a composite of the online SaaS agreements surveyed.¹⁰

Sellhard.com's subscription agreement grants a non-exclusive, non-transferable, worldwide right to use the service. Payments are due in advance for a license term. Users owe for all individual licenses regardless of actual use. If users violate terms, their access is terminated without refund. Licenses are automatically renewed unless users notify Sellhard.com, but the deadline for giving legal notice of non-renewal is ill defined in the document.

The above terms sound more like a software license than an access agreement. In essence, the terms provide a right to use software subject to prepayment for a length of time spanning years. The terms give Sellhard.com unabated power to take away the right to access the service without having to prove that violations have taken place or providing any opportunity for customers to explain. This feature of the agreement is equivalent to the UCITA self help provision discussed earlier, which gave software vendors the right to remotely disable software.

Like licenses, Sellhard.com's agreement addresses permitted and prohibited uses of the accessed software. In perpetual software licenses, prohibited uses mostly have to do with unauthorized copying, e.g., too many

¹⁰ Any resemblance between the fictitious SaaS provider named Sellhard.com in this white paper and any individual actual provider is coincidental and unintended. The composite services agreement used in this white paper is not intended to represent all SaaS providers.

users, too many installs, installs on unauthorized networks. Only a handful of terms "characterize" prohibited uses of software, i.e., do not use the software in a service bureau setting, do not use the software in inherently dangerous activities such as nuclear power plants.

By eliminating the existence of copies and installs of software, SaaS should eliminate most if not all chances that customers will violate user terms and breach the contract. If SaaS ever morphs into the utopian version of utility computing, the concept of right or wrong ways of using the service would become meaningless, and only fraudulent access or failure to make timely payment could constitute a violation.

But our fictitious Sellhard.com agreement goes to great length in prohibiting customer use by characterizing numerous ways the service cannot be used. The Sellhard.com agreement terminates service for committing any of a long list of offenses. Users are prohibited from doing any of the following: monitor the services' availability, functionality or performance; hyperlink to the service or mirror it on a network; build a similar service; spam, send viruses, or store or send harmful material including to children; disrupt the service or try to gain unauthorized access. The first offense listed, that of benchmarking the service, once again brings up UCITA. One UCITA provision that was designed to protect consumers was Section 105(c) outlawing contract clauses prohibiting criticism of software performance.¹¹ On this count the

¹¹ Section 105, Uniform Computer Information Transactions Act, Amended 2002, National Conference of Commissioners on Uniform State Laws.

Sellhard.com agreement fails to meet the standards of a model law that was heavily criticized for being pro-industry.

Other language in the agreement says users cannot: make the service available to any third parties; modify or make derivative works from the service or build competing services; or copy any ideas, features, functions or graphics. Any user feedback on the service becomes Sellhard.com's property. This language addresses the legal issues of infringing on patents and copyright (ideas are patentable; derivative works is one of the rights in a copyright). But since Sellhard.com is a services provider, not a licensor, the wording might be used by Sellhard.com to prevent customers from replacing Sellhard.com's service with either an on premise system or a competing system that provides better functionality, in essence creating an exclusive supplier provision. Sellhard.com seems to be reaching here for some of the same protections it would enjoy as a software licensor, but in doing so Sellhard.com places potentially enormous risks on customers that go beyond access itself.

So far, Sellhard.com's service terms do not sound attractive if you are a business looking to purchase a software system. Sellhard.com's agreement raises the question of whether Sellhard.com is being commercially reasonable. It's hard to say. That's because of the fundamental difference between traditional software licenses and SaaS. While licenses are grounded in intellectual property law, as discussed above, SaaS is based on use of the Internet. There are many more ways to characterize using the Internet than there are ways to characterize using intellectual

property. So Sellhard.com's subscription agreement, or any other SaaS agreement, potentially imposes many more restrictions on customers than would a license, creating greater risk for customers.

SaaS users must also concern themselves with how the Internet use laws apply to them and how their potential legal liability is addressed in SaaS services agreements. Use, access, storage, transmission, posting, backups, security, law enforcement, record keeping and backups are all actions done by Internet users that are subject to laws.¹² Sellhard.com's contract places responsibility on customers to comply with all state, national and foreign laws regarding data privacy and transmission of data, exacerbating the customer's potential risks.

One major difference between the Sellhard.com agreement and traditional licenses is Sellhard.com can change any term in its contract without notice by posting new terms online without notice and requiring users to constantly revisit the site, reread the terms and interpret whether any changes have been made. License terms by nature do not change unless the changes are mutually agreed to by amendment. Also licenses usually cover future updates in addition to the current version number of the code. The idea of vendors unilaterally changing terms was another UCITA section that garnered a lot of bad publicity.¹³ The Sellhard.com agreement may appear less

¹² A discussion of particular statutes and law governing SaaS services is outside the scope of this white paper.

¹³ Section 304, Uniform Computer Information Transactions Act, Amended 2002, National Conference of Commissioners on Uniform State Laws.

unfair than UCITA because Sellhard.com thinks of itself as a service. The consequence, however, is equivalent to UCITA.

Data and SLAs

The above comparison still hasn't reached the most troublesome subjects for SaaS as compared to software: the ownership, possession and control, and safeguarding of data; and the guarantee of network service levels.

Software licenses don't discuss data except for waiving any vendor liability for consequential damages to customer data caused by software processing errors. It's a sensible position for software OEM's to take, given that customer data doesn't pass through their hands. If consulting services are being provided in addition, OEM's typically will place a cap on their liability for data damaged by personnel and protect themselves with errors and omissions insurance.

The SaaS model turns the relationship between customers and their data on its head. Besides providing access to applications, a SaaS service includes storage of and access to customer data. Stored data is physically located on premises operated by the SaaS company or by a hosting company under contract with the SaaS. Likewise, with a SaaS service customer, data is stored on the SaaS company's hardware or the SaaS host's hardware, and is maintained by SaaS personnel, the host's personnel, or some third party IT maintenance company.¹⁴

¹⁴ A number of industry terms have come into being over the years to describe the different permutations

Sellhard.com's agreement provides that customer's must receive permission to remotely access their data. No other method of access during the term of the contract is mentioned, such as requesting a copy in database form. Nevertheless, customers are deemed to "own" the data. Customer ownership is not dependent on whether customers actually create the data or possess it any time during the service term. Nor do Sellhard.com's terms address third party rights in data in any way. What if third parties, namely the customer's customers, are the actual users of the service or create the data in a separate program? They would do so without ever entering into any formal relationship of any kind with Sellhard.com.

Sellhard.com takes no responsibility for customer data integrity, confidentiality or security. In fact Sellhard.com can immediately destroy the data without notice if it believes the customer has violated service terms. Sellhard.com is also not required to delete any customer data in its possession and is not liable for unauthorized disclosure of the data, raising concerns of resale or inadvertent access by competitors. This is not an academic point. In a famous 1994 Massachusetts legal case, TRW, a credit bureau, ended a contract with another credit bureau supplying data. TRW ignored a clause in the contract requiring it to destroy the data. TRW attempted to get around the clause and retain the data for its own use by reasoning that the data was already public.¹⁵

of hosted software including collocation, managed services, and ASP.

¹⁵ Credit Data of Central Mass v. TRW, 37 Mass. App. Ct. 442 (1994).

Sellhard.com addresses data security concerns in an online security statement. The statement explains that the latest server authentication and data encryption technology are used to protect data, but no independent standards, auditing or testing are mentioned.

The upshot of Sellhard.com's contract language on data is Sellhard.com places all responsibility for data entirely with the customer, while giving the customer no real way of exercising the imposed responsibility.

The greatest shock in reading Sellhard.com's contract comes from discovering the absence of any network service levels. The agreement terms portray the Internet as a kind of wilderness which Sellhard.com can't control. Specifically the agreement says the Internet has inherent limitations, delays, and other problems for which Sellhard.com is not liable.

Strictly speaking, a SaaS agreement disclaiming any service level is equal to a software license refusing to guarantee delivery of a complete application. Nor does the absence of any SLA meet industry standards. As a rule, network and Web hosting services guarantee at least 99.9% 24x7x30 uptime and escalate resolution of outages. Business continuity and disaster resolution are completely outside Sellhard.com's business model.

Sellhard.com's one way definition of data rights and responsibilities, and its lack of an SLA, are both major drawbacks for any SaaS offering. If SaaS providers intend to fulfill the goals of lessening customer risk and improving ROI over that of licensing,

then SaaS data rights and duties of care need to be more precisely defined by contract. In the same vein, SaaS providers and network service providers need to work out contractual SLAs. The SIIA has taken one step towards addressing the service level issue by drafting a model SLA provision including credits for service failures.¹⁶

SaaS Business Chain Links

The SaaS data and SLA hurdles point to another fundamental difference between the SaaS and software license models, namely that SaaS necessarily involves more interested parties and more potential legal relationship issues, regardless of the existence of formal contracts. SaaS providers, hosts, network service providers, third party "ecosystem" application vendors, customers and users become links in a legal and business chain that may never be completely joined in a SaaS transaction. Resellers of SaaS add another link to this chain. A license on the other hand is mostly a transaction between two parties. Potential approaches to overcoming the data and SLA hurdles include SaaS providers becoming "aggregators" that bear ultimate responsibility for data and service levels, or conversely, SaaS providers directing customers and users to sign separate agreements with third parties providers such as data vaults and networks.¹⁷

¹⁶ "Setting Expectations in SaaS: The Importance of the Service Level Agreement to SaaS Providers and Customers" (February 2007, SIIA Executive Council on Software as a Service).

¹⁷ A James River Consulting will publish a white paper analyzing the various roles and relationships comprising SaaS in Fall, 2007.

Data Privacy and Data Compliance Value Add

One enormous value proposition offered by the SaaS model not mentioned in Sellhard.com's terms is the growing administrative burden of housing data. It is a value proposition with which the software licensing model cannot compete.

Besides compliance with privacy and security standards like Sarbanes-Oxley, SAS-70 and HIPPA, a large body of laws has evolved requiring data custodians to respond to notices, subpoenas, warrants and court orders effecting data in the form of copyrighted material, communications contents and transmission, and subscriber records. Data custodians are legally bound to cooperate with copyright owners and Government regulatory and law enforcement agencies. Associated costs are not necessarily reimbursed. Violators are subject to both civil suits and criminal prosecution.

Two immediate and daunting concerns faced by companies and institutions that house data are the tricky disclosure rules of the Stored Communications Act and the political push in both Europe and the United States for "data retention" statutes. While these laws are aimed at ISPs, they also apply to SaaS providers.

The Stored Communications Act (18 USC 2701 et. seq., part of the Electronic Communication Privacy Act (ECPA)) in a nutshell prohibits "remote computing service" providers from disclosing content which is protected by the 4th Amendment right of privacy, and subjects providers to law suits for monetary damages if the rules in the Act are not followed properly.

Unfortunately for providers, the rules are complicated and do not clearly apply in many situations. A 2004 federal District Court case highlights the precarious position of CIOs under the ECPA. In 2004 an AOL subscriber named Clifton Freedman successfully sued AOL for emotional distress and damage to his public reputation using ECPA's civil liability provision. An AOL employee had disclosed Freedman's identity and an email he sent in a political campaign; the data was disclosed in response to a warrant faxed to AOL by the Fairfield, Connecticut police. Warrants are an exception to liability in the Act. But the warrant in the Freedman case had an illegible signature near the judge's signature line that turned out to be one of the detective's, not the judges, making the warrant invalid. Even though AOL was responding to 1,000 warrants for data a month, and had a dedicated staff for responding to data request, and despite the honest mistake made by the AOL employee, the court found AOL liable.¹⁸

Exacerbating ECPA's trickiness and further increasing the difficulty and cost of complying with ECPA, on June 18, 2007, a federal Circuit Court ruled that some of ECPA's rules for what is and isn't a valid court order for data are unconstitutional for content type data. Contrary to language in the Act allowing law enforcement to make warrantless requests for data, the court said ISPs cannot turn over emails to the Government without a warrant or without the ISP appearing in court to show that

¹⁸ Freedman v. AOL, 325 F.Supp.2d 638 (E.D. VA 2004); Reconsideration Denied 329 F.Supp.2d 745

emails are not private given how the service operates.¹⁹

Data retention is another recent development that already has created added costs for data housing. The European Commission passed a Directive requiring public electronic communications services and providers to store certain data for periods ranging from 6 months to 2 years.²⁰ In the US, Attorney General Alberto Gonzales has publicly called for data retention laws in the United States and in private has met several times with major US ISPs about voluntarily preserving data for up to 2 years. In February of 2007, the Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2007 (SAFETY Act) was proposed in Congress, which would require ISP's to store certain data for 2 years. The Stored Communications Act already empowers Federal prosecutors to request remote computing providers to "preserve" data up to 180 days, without court order (18 USC 2703(f)).

¹⁹ Warshak v. US, No. 06-4092, Decided June 18, 2006, US Court of Appeals for the 6th Circuit.

²⁰ DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC



James River Consulting

Better IT Contracting

www.jamesriverllc.com

**134 Hillside Avenue, Needham, MA 02494 703.850.7061-Mobile
info@jamesriverllc.com jamesriverconsulting@comcast.net**



ABOUT THE AUTHOR

Eric Esperne is president of James River Consulting based in Needham, Mass., a new consulting company specializing exclusively in IT contract development, negotiation and performance management. Prior to creating James River, Eric served as a senior in-house counsel, general counsel, director of contracts, senior strategic software procurement leader and Internet product development leader for multi-national telecoms and government and commercial IT vendors in and around Washington, D.C. He can be contacted at eesperne@jamesriverllc.com or 703.850.7061.