DOING BUSINESS ONLINE

LEGAL ISSUES IN THE UNITED STATES

06 APRIL 2018

The United States has a well-developed set of practices and common terms related to technology and Internet contracts. Some are complex and include traps for the unwary. Even if you have a lawyer's help, you will fare better with an understanding of the key concepts. This document outlines nine key contract issues. It also describes the supporting documents typically included with online contracts, and it offers a brief explanation of US intellectual property.

KEY CLAUSES/CONCERNS IN TECHNOLOGY AND INTERNET CONTRACTS

IP indemnity

US customers generally expect their vendors to indemnify them against IP suits – third party claims that the customer infringed IP by using the vendor's technology. But an IP indemnity can run the other way. In software-as-a-service (SaaS) deals, where the customer puts content or data on the vendor's computers, vendors sometimes demand an indemnity too. In these 'content indemnities', the customer indemnifies the vendor against suits claiming the hosted data infringed third party rights. Indemnity terms are usually complex and riddled with exceptions – and often poorly understood – so negotiations may move slowly.

Personal injury and data breach indemnity

In American contracts, one party often indemnifies the other for claims of harassment or physical injury resulting from meetings between the two parties' employees. These personal injury indemnities rarely delay negotiations, but data breach indemnities do. Customers want SaaS and other cloud vendors to indemnify them against privacy suits related to data breach. But vendors worry that customer error could cause a leak, even though the vendor hosts the data. So, they resist granting an indemnity and may even ask to receive one. Unfortunately, US industry has not settled on a common practice, so again, negotiation delays are common.

Ownership and control of data

Control of data now plays a central role in American technology contracts. Often, one party claims to 'own' data. But American law does not actually allow clear ownership of information. Copyright and other IP ownership concepts may play a role in data rights, but instead of relying entirely on ownership, focus on who controls data. Who has the right to copy it, move it or change it? And who controls 'derived data' – information generated by analysing the data? Many contracts also address control of 'aggregate' or 'anonymised' data. Cloud vendors often want the right to reuse or sell their customers' anonymised data.

Australian Government
Australian Trade and Investment Commission

Australia UNLIMITED

Data security

Some American technology contracts still use nondisclosure agreements (NDA) and similar confidentiality terms to address data security. That's a mistake. Real data security clauses address data protection procedures for SaaS vendors and other data holders. Topics include encryption, location of data, employee background checks, and data breach response. Data clauses may also address 'e-discovery.' The US legal system restricts the right to change or delete data during or in advance of litigation, to preserve electronic discovery, so customers need to make sure vendors holding their data comply with e-discovery requirements. Data security clauses also address compliance with law, to ensure that the vendor won't put the customer in breach of US or international privacy laws. Finally, American data security clauses often require regular audits of the vendor's data security systems, called SOC–1, SOC–2, and SSAE–16 audits – names based on standards from the American Institute of Certified Public Accountants (for sample data terms, see section II-H at the linked page).

Limits of liability

Limits of vendor liability are nearly universal in American technology contracts. They cap vendor liability at some dollar amount and limit the customer to direct damages (the normal, predictable loss from technology failure) and exclude consequential damages (the unique consequences of a particular failure). Customers generally accept these restrictions, but the dollar cap amount is often negotiated. There is no magic number, but one year's fees is common. Try not to argue about the 'fair' amount of a dollar cap, since the figure is arbitrary. Finally, customers sometimes insist that the limit of liability protect them too. If the vendor accepts, it should at least make sure customer liability for IP infringement is *not* limited.

Non-compete and non-solicit

US law restricts non-compete agreements. If one party promises not to compete with the other, both risk legal action for antitrust violation. Limited restrictions on competition are possible, but you should always get a lawyer's help. Non-solicit clauses are safer, though legal advice is still a good idea. One party agrees not to poach the other's employees, often in a professional services agreement. Some US states restrict non-solicit clauses too, generally to protect the employee. Non-solicits work best if narrowly crafted, with limited durations and limited employees impacted.

Technology escrow

Software escrows appear in US license agreements where the customer fears the vendor will go bankrupt and so stop providing support. The parties place the vendor's source code with an escrow agent, to be provided to the customer after a bankruptcy. You should use an established escrow company that can protect the source code and test to confirm that it can be compiled into machine-readable code. Escrow does not work for SaaS and other cloud-computing deals, where receiving source code from an escrow agent would do the customer little good. To run the SaaS/cloud system, the customer would need to replicate the vendor's whole infrastructure – including servers, data centre, and supporting software. Customers should consider an alternative – 'step-in rights', where the customer gets to 'step in' to the vendor's relationship with its data centre and take over the computers if the vendor goes bankrupt.

Clickwraps and unilateral amendment

Internet companies often post their contracts for online signature, and American courts have found these 'clickwrap' contracts enforceable. But one common feature of the clickwrap probably is not. Many say the vendor can amend the terms without notice or consent from the customer. American courts have held that these unilateral amendments are not binding. And one court suggested a unilateral amendment clause might invalidate the whole contract. So make sure your amendment terms give customers notice and the chance to consent, or not, as in this example.

Choice of law

A widespread myth says Delaware is a neutral or ideal state for a contract's choice of law and courts. Delaware has advantages for corporate law, such as incorporation and deals among shareholders, but not for commercial

contracts, like technology and Internet agreements. Another myth says California law is dangerous. California has unusually strong employee and consumer protection laws, but they play little or no role in deals between companies (California also has more tech companies than any other state, and they tend to favour their own laws and courts, even for consumer and employee relationships). In general, companies should choose the law and courts of their home state. 'Forum shopping' takes a lot of legal research and often backfires.

SUPPORTING DOCUMENTS FOR ONLINE CONTRACTS

Privacy policy

Some US states require a privacy policy, so you should always have one, since you may have customers in those states. A privacy policy should be an honest disclosure about personally identifiable information (PII). At a minimum, it should disclose:

- the type of PII collected
- the types of third parties who get access to PII
- how PII is used
- security measures to protect PII (summarised)
- how users can review or change their PII
- how the vendor notifies users of privacy policy changes
- the effective date of the policy.

Acceptable use policy

The acceptable use policy (AUP) forbids harassment of other users, spam, offensive language, and the like. It sometimes also restricts IP infringement. Vendors need this policy only if customers can actually do these things – if the service includes communications or content-posting systems. Here is a sample policy.

DMCA policy

The Digital Millennium Copyright Act (DMCA) lets online service providers escape liability for their customers' copyright infringement. To take advantage of it, companies must:

- make sure they don't block technical used to detect infringement
- register an agent with the US Copyright Office
- post that agent's contact information online
- enforce a policy of terminating repeat infringers
- follow a set of statutory procedures related to notice of infringement and, in some cases, removal of content.

The DMCA policy itself is just an online notice: 'For claims of copyright infringement, please contact _____ [insert agent's contact information]. We will terminate the accounts of subscribers who are repeat copyright infringers'. But some companies add details of the statutory notice and takedown procedures – as in this example notice.

SLA

A service level agreement (SLA) is not an agreement but rather a contract clause. The vendor promises to fix failing SaaS or other cloud services – and sometimes offers credits for failures. Many US companies post SLA's online.

INTELLECTUAL PROPERTY

The human creator of IP owns it under US law, but companies generally own IP created in their employees' scope of work. Just to be sure, sign IP assignment agreement (like this example agreement) with any employee likely to create technology or important content.

Contrary to common belief, no one can own an idea in the United States (or in most countries). If you have an idea for a new product, feature, or business, or a new technique, everyone can use it (if they find out about it legally). You can own a 'mental asset',

however, if it qualifies for one of the following categories.

Copyright

This is a monopoly on an original work of authorship fixed in a tangible medium – like software, a book, a photo, a video, or the shape of a statue. Copyright covers the expression, not the underlying idea. So copying software or a book infringes copyright, but writing independent software or text using the copyright holder's ideas does not. In the US, copyright exists as of creation, but it's easier to enforce if registered with the Library of Congress.

Patent

A patent is a monopoly on an invention or design. Some software can be patented, but an idea cannot. The patentee must invent or design something. Patents must be filed with the US Patent and Trademark Office.

Trade Secret

This is information that is both:

- valuable because it is not widely known
- subject to reasonable efforts at secrecy.

If a third party uses a trade secret gained without authorisation, it can be liable to the trade secret holder. But if the information gets out through the holder's failure to protect it reasonably, anyone can use it.

Trademark

A trademark is a name, logo or similar identifier that announces the source of goods or services. If the mark is distinctive and used in commerce, the owner can keep others from using it. Trademarks do not have to be registered, but they're easier to enforce if they are. Most states offer registration, but the federal Patent and Trademark Office gives broader protection.

DISCLAIMER

While care has been taken to ensure the information in this document is accurate, the Commonwealth of Australia represented by the Australian Trade and Investment Commission does not provide warranty or accept liability for any loss arising from reliance on such information.

Prepared by David W. Tollen
david@SycamoreLegal.com

Sycamore Legal, P.C.
https://www.sycamorelegal.com

Tech Contracts Academy,
San Francisco, CA
https://techcontracts.com