

# Business Insider

Spring 2007 Edition

## **This Edition:**

- Pg 1 Doing Business On The Web - Clickwrap Agreements  
Pg 2 Computer Fraud And Abuse Act  
Pg 3 Establishing Patent Priority For Interfering Patent Applications

## ***DOING BUSINESS ON THE WEB - CLICKWRAP AGREEMENTS***

Every day, more and more business transactions are conducted over the Internet. Many of these transactions begin with a “clickwrap agreement.” Clickwrap agreements are variations on “shrinkwrap” agreements, those printed terms and conditions usually found in the packaging for software. Clickwraps basically work the same way, but the user agrees to the terms by clicking a button on his computer, instead of by opening the package and using the product. While clickwrap agreements are still widely associated with software licensing, their use has spread to a wide range of business settings, such as advertising services, telecommunications, and banking, to name a few.

Given that clickwraps have become ubiquitous, it is prudent for businesses to consider their advantages and to be informed as to the desirable characteristics that any clickwrap agreement should have. As compared with their paper predecessors, clickwraps are easier and quicker for a customer to accept, and more difficult for the customer to attempt to change. They provide a measure of control that is to the business’s advantage. Depending on the size of the business and its market, clickwraps can be the means by which countless relationships are formed and deals are struck, so it is vital for any business using them to get all of the details correct. To ensure enforceability and to head off later legal problems to the greatest extent possible, companies should seek and use the advice of legal counsel as they create clickwraps tailored to particular businesses.

Once a business decides to use a clickwrap agreement, there are certain traits that should be considered:

- *Put the steps in the right order.* Before a customer is expected to pay for the product or service, or is allowed to receive it, he should be given the chance to review the entire clickwrap agreement and the option to accept or reject all of its terms and conditions.
- *Identify the user.* If the party who comes to a company’s clickwrap represents another company, it is especially important to get identifying information that will show that the user is authorized to bind his company to the agreement. To this end, the clickwrap should have places for the user’s name, the company’s name, the user’s title, and both e-mail and physical addresses. Of course, aside from its value for such verification purposes, the identifying information can be useful in other ways.
- *Do not make the user hunt.* The clickwrap should be readily apparent to a user, and the “install” or “download” button should appear only after the clickwrap is set out in its entirety. In the same vein, a checkbox indicating that the user has agreed to the terms of the clickwrap makes good sense. The idea is to prevent anyone from claiming in a later dispute that there were parts of the agreement that he could not have easily seen, and to

which he did not give his assent. As for any terms that are weighted in favor of the business, making them hard to find is an especially bad idea. On the contrary, these terms should stand out, maybe even with their own “I agree” checkbox.

- *Drop the legalese.* As is true for any contract, a clickwrap should use clear, plain English. It is well settled in law that a court will construe ambiguous terms against whoever wrote them, that is, the business whose clickwrap is being deciphered.
- *The clickwrap should control.* If there are any other dealings with the user, whether oral or written, that conceivably could be said to constitute a separate agreement, they all should explicitly defer to the clickwrap agreement. Likewise, the clickwrap itself should have language indicating that its terms override any conflicting terms in other agreements relating to the transaction.

- *Keep the final word.* What if a user navigates successfully and accepts the clickwrap agreement, but your business determines for some reason that it wants no business relationship with that user? The business should provide itself with an escape hatch, with language in the agreement to the effect that the business must confirm the agreement before it becomes enforceable, or that the business can cancel the agreement at will.

Clickwrap agreements have gained acceptance as valid, enforceable contracts, albeit in an unconventional format. This point is illustrated by a recent federal court decision. In a breach of contract dispute between two software companies concerning the use of licensed software, the court hardly paused at the question of whether a clickwrap agreement constituted a valid contract. In answering “yes,” the court also relied on an extensive list of prior court decisions that had reached the same conclusion. The clickwrap agreement has become a permanent part of the legal landscape for businesses and individuals alike.

## **COMPUTER FRAUD AND ABUSE ACT**

Since 1994, the federal Computer Fraud and Abuse Act (CFAA) has provided civil remedies to complement the original criminal sanctions for the theft and destruction of computer data, fraudulent use of passwords, and various means of committing fraud by unauthorized access to computers. For a typical claim under the CFAA brought against a defendant who violates the statute in an attempt to gain a competitive advantage over the plaintiff, there must be a financial loss of at least \$5,000 in order to maintain a civil cause of action.

The ability to obtain injunctive relief under the CFAA is at least as valuable to an injured party as the recovery of damages. To win an injunction, however, the plaintiff must be in a position to prove not just the unauthorized intrusion into the plaintiff’s computers, but also specifics as to what information was taken by

the defendant and how it was used to harm the plaintiff.

In a recent case, a former officer and an employee of a party supply store were alleged to have gathered information from their former employer’s computer without authorization, so as to get a leg up on the plaintiff in their new, competing business. The elements for the claim were in place, except for the critical proof as to what data records of the plaintiff’s were accessed and whether such records had been downloaded, copied, or printed by the defendants. The plaintiff business was denied an injunction in federal court because of this gap in its proof.

The case of the competing party supply businesses offers object lessons for how businesses can best put themselves in a position

to take full advantage of the Act if they have been victimized. One advisable technical step is to include an auditing function in a computer system that automatically records what documents have been accessed and what happens to the documents when they are accessed. The resulting “audit trail” can be a valuable piece of evidence in an action under the CFAA. When employees are allowed to work at home on their computers, employers should have policies allowing them to inspect those computers when the employment ends and to retrieve any of their data.

Although technical measures and policies on computer technology are important, simple use of imagination can also produce relevant non-computer evidence for a CFAA claim. The court in the unsuccessful action by the party supply store observed that the plaintiff could have presented evidence that the defendants had taken particular actions to the competitive disadvantage of the plaintiff very soon after their unauthorized access to the plaintiff’s computers. This would have allowed an inference that secrets had been taken from, and then used against, the plaintiff.

### ***ESTABLISHING PATENT PRIORITY FOR INTERFERING PATENT APPLICATIONS***

Under the United States patent system, patents are awarded to inventors who are the first to invent, as opposed to the first to file a patent application. Unless another inventor can show that he conceived of an invention first, and was reasonably diligent in later reducing the invention to practice, the inventor who first reduces the invention to practice is entitled to the patent. “Reduction to practice” can be either constructive, such as by filing a patent application, or actual, such as by constructing a working model or prototype of a product, carrying out the steps of the invented method, or producing the composition of an invented material.

In litigation over competing, sometimes called “interfering,” patent applications for the same invention, evidence of actual reduction to practice is pivotal in establishing the priority of an invention. Such evidence is the “meat on the bones” of a legal case for establishing priority in an interference proceeding. The winning party will have to show that it constructed the claimed embodiment or performed the claimed process, that the embodiment or process functioned for the intended purpose, and that there is sufficient evidence to corroborate the inventor’s testimony as to the first two requirements.

The importance of unassailable evidence of reducing an invention to practice is illustrated by a case in which two companies were competing for a patent for making an active ingredient in an

allergy medication. Neither party relied on a date of conception, so the case turned on who first reduced the invention to practice. One company had the earlier filing date on its application, but the second company claimed that it had earlier reduced the invention to practice.

Given the subject matter of the invention, the second company’s evidence was in the form of laboratory data and notebooks kept by individuals closely associated with the inventive process. Unfortunately for that company, flaws in this evidence greatly diminished its weight and led the court to rule in favor of the first company. Essentially, the evidence lacked sufficient corroboration, such as by signing notebooks, using witnesses to vouch for their authenticity, or having individuals testify as to the genuineness of the notebooks’ contents. Such shortcomings likely would have been enough by themselves to tip the balance, but evidence of fraudulent backdating of notebook entries was another fatal blow to the second company’s case.

#### ***Make Sure to Carefully Document Evidence***

There is no single, exclusive method for marshaling and authenticating evidence for use in a patent priority battle, but the case of the allergy medication ingredient suggests that a meticulous approach is prudent. Examples of practices that should be in place include bound

notebooks for inventors, with each page signed and dated in permanent ink not only by the creator of the notebook, but also by a disinterested but informed non-inventor; placement of entries in chronological order; and initialing and dating of any corrections. Inventors should record as much detail as possible about their activities and conclusions relating to the invention, and there should be a full explanation for any supplementary materials. Finally, all of this attention to detail and following of procedures could be for naught

unless the information is kept in a secure place to which there is authorized access only.

Just as scientific methods must be followed in the very work that leads to a patented invention, a company should adopt and rigorously follow procedural guidelines for recordkeeping in connection with any of its work that could lead to a patent. Otherwise, there is a great risk of wasted effort and the loss of what could be very valuable intellectual property.

---

*The Business Insider newsletter is provided as a general informational service to clients and friends of Tinovsky Law Firm. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does it create an attorney-client relationship.*

*For more information, please contact **Vlad Tinovsky, Esq.** at [vtinovsky@tinovsky.com](mailto:vtinovsky@tinovsky.com) or **215.568.6862**.*

© 2007 Tinovsky Law Firm. All Rights Reserved.