ARE CONSUMER NOTICES AND USER AGREEMENTS RECEIVING PROPER ATTENTION?

By Glenn J. Light, Kade D. Miller and Karl F. Rutledge

The Internet has allowed operators to reach countless new customers and expose their products and services in ways unimaginable only decades ago. With such widespread dissemination, however, also comes more potential challenges and pitfalls. This article explores the importance of Terms of Use, End User License Agreements and Privacy Policies for online operators. Each of these agreements serves a special purpose that companies with online operations should be mindful of, and this article expounds upon these agreements with the aim of keeping you and your online business protected.

Terms and Conditions & End User License Agreements

Terms and Conditions, which are sometimes referred to as Terms of Service or Terms of Use, are, in essence, a contract between an operator and a user that governs the use of the operator's website. A link to the Terms and Conditions is often found in a banner at the bottom of the website with links to other information such as the operator's Privacy Policy (discussed below) and contact information. In contrast, an End User License Agreement is a contract between an operator and a user that establishes the user's rights to use certain software that he or she has downloaded. Due to similarities between these documents and the contents they govern, if a user is able to download software, the End User License Agreement typically forms part of the Terms and Conditions.

As every business is different, Terms and Conditions and End User License Agreements should vary depending on the purpose of the business, the purpose of its website and/or the purpose of its software. For instance, when an operator approaches its Terms and Conditions, it should consider a number of factors, including:

- the website's main purpose;
- the services offered on the website, (e.g., information, products, entertainment);
- where the services are offered;
- the rights a user grants to the operator by posting pictures, videos, comments or other works on the website;
- how the operator deals with online orders, deliveries and returns;
- how and where the operator settles disputes;
- how the operator protects its intellectual property and intends it to be used;
- how users are expected to behave on the website's online forums; and
- possible problems a user could encounter while using the site.

If an operator fails to give the necessary credence to applicable factors and instead opts to use a generic document, an operator exposes itself to unnecessary liability. Off-the-shelf Terms and Conditions or End User License Agreements undoubtedly will include irrelevant provisions, and worse yet, provisions that work against or fail to protect the operator's interests.

In addition to being company specific, Terms and Conditions and End User License Agreements should be drafted and presented in a clear and coherent manner to ensure their enforceability. Furthermore, a user's acceptance of Terms and Conditions and End User License Agreements should require affirmative consent. A popular methodology for obtaining a user's affirmative consent is to require each user to click "I Accept" or a similar link, commonly known as "clickwrap," to evidence their acknowledgment and assent to the Terms and Conditions and End User License Agreement.[1] If the Terms and Conditions or End User License Agreement is incomprehensible or lacks sufficient evidence that users have read and accepted such terms, there is an increased risk that a court will find the document unenforceable due to the absence of user assent.

This risk became increasingly apparent in 2012 when a Nevada court held that Zappos.com's Terms and Conditions were illusory and therefore unenforceable.[2] In mid-January 2012, Zappos' computer system experienced a security breach in which hackers attempted to access the company's user accounts and personal information. After Zappos notified its users about the incident, users from across the country filed lawsuits against Zappos seeking relief for damages arising from the breach. Zappos sought to enforce the arbitration clause contained in its Terms of Use, which would stay the litigation in federal court and compel the case for arbitration. Zappos contended that users had consented to its Terms of Use, which were amended to include an arbitration clause, by merely posting the amended terms on its website in a manner commonly known as a browsewrap agreement. The court contrasted Zappos' "browsewrap" agreement against a clickwrap agreement and found that Zappos' Terms of Use were unenforceable because there was no evidence that users consented to or even had actual knowledge of the terms, including the arbitration clause.

Not all jurisdictions follow the precedent set forth by the Nevada federal district court.[3] Nevertheless, a prudent online operator will be mindful of such requirements or limitations imposed by consumer

friendly jurisdictions and tailor its agreements and procedures accordingly.

Privacy Policy

While the protection and integrity of the website is essential, the protection of a user's personal information is equally crucial. A Privacy Policy is a legal notice detailing what information an operator will collect and how that information will be collected, used and stored. Similar to Terms and Conditions and End User License Agreements, an operator must take the time to draft its Privacy Policy in a manner that is clear, precise and specific to its handling of user information.

When an operator approaches its Privacy Policy, it should consider a number of factors, including:

- the information collected;
- the method of collection (e.g., directly from users, from other sources);
- how the information is stored and protected;
- how long the information is maintained;
- how the information is used; and
- with whom the information is shared.

For instance, an operator will typically collect both personal and general information about a user. Personal information is information by which a user may be identified. Examples include first and last names, addresses, telephone numbers, email address, cell phone numbers and credit card information. General information is information about a user and his/her activities on the website that does not identify the user personally. Examples include a user's domain server, type of computer, web browser, operating system or platform, cookies, movement and activity within the site, as well as other webpages visited by a user. A Privacy Policy should specify the types of personal and general information collected by the operator. In addition, operators routinely share user information with affiliates, partners and other third parties. In such instances, an operator's Privacy Policy should specify the information shared, with whom it is shared, and how the recipient handles such information.[4]

Like Terms and Conditions and End User License Agreements, an operator's Privacy Policy is not a static document but must be periodically updated to reflect changes to the operator's practices and technology, and to comply with new legal requirements. A significant change that recently occurred in California involves amendments to the state's Online Protection Act. Under the amended law, Privacy Policies must provide two additional disclosures. First, if an operator collects personally identifiable information about a user's online activities, including those across third-party websites or online services, the Privacy Policy must include information about how the operator responds to "do not track" signals or other mechanisms that provide users with a choice regarding the collection of their personal information. Second, Privacy Policies must state whether other parties may collect personal information from a user when he/she uses the operator's website or services. Although the recent amendments apply only if the person visiting the website is a California resident, residence is not an easily identifiable trait. Accordingly, absent compliance with the new Privacy Policy requirements, an operator risks liability under California law.

In addition to obtaining initial consent from users for the Terms of Use, End User License Agreement and Privacy Policy, an operator also must ensure that any subsequent changes it makes to these agreements are binding. The continued use of a website is erroneously assumed by some operators to constitute sufficient assent to the changes. Similar to obtaining initial consent, best practices dictate that an operator should obtain the users' express acceptance of the changes, i.e., requiring users to provide affirmative assent to the new policies the first time the user visits the site or logs on to the site after the changes take effect, as opposed to trying to surmise assent based on a user's failure to object or challenge the new policies. While requiring affirmative assent is not required in all jurisdictions, anything less than such assent in the more consumer protective states raises concerns.

In summary, online operators should acknowledge the increased scrutiny given to Terms of Use, End User License Agreements and Privacy Policies. Most notably, operators must not only appreciate the need to clearly and accurately detail their policies and the information collected from users but also understand how to ensure such policies are enforceable.

If you have any questions regarding these agreements or how they may be of benefit to your online operations, please do not hesitate to contact the authors.

1 As noted above, both documents are essentially a contract, and the formation of any contract requires both an offer and acceptance With regard to Terms and Conditions, the offer is made by the operator, which offers the services on its website, and the acceptance is made by the user, who accepts to be bound by the terms. Similarly, with regard to End User License Agreements, the offer is made by the operator, which offers the user the right to use certain software, and the acceptance is made by the user, who accepts to be bound by the terms of the End User License Agreement.

2 In re Zappos.com, Inc. Customer Data Sec. Breach Litig., 893 F.Supp.2d 1058 (D.Nev.2012).

3 Damato v. Time Warner Cable, Inc., No. 13-CV- 94, 2013 WL 3968765 (E.D.N.Y. July 31, 2013).

4 Special consideration must be given to information that is collected from children under the age of 13, as this information triggers compliance with the requirements set forth in the Children's Online Privacy Protection Act (COPPA). The provisions of COPPA are far reaching and apply to any online operator with knowledge that it is collecting personal information from children under 13, as well as operators of child-directed websites that integrate outside services, including plug-ins and advertising networks that collect personal information from its visitors. Given the audience of this article we have not addressed the COPPA considerations but if you have any questions regarding COPPA please feel free to contact us.

GLENN **LIGHT**

Glenn Light is an attorney in the Gaming Practice Group in the Las Vegas office of the law firm, Lewis Roca Rothgerber LLP. His practice focuses on casinos, horse racing, sports betting, Internet gaming, sweepstakes and contests. He may be reached at GLight@LRRLaw.com.

KADE **MILLER**

Kade Miller is an attorney in the Gaming Practice Group in the Las Vegas office of the law firm, Lewis Roca Rothgerber LLP. He may be reached at KDMiller@LRRLaw.com.

KARL **RUTLEDGE**

Karl Rutledge is a partner in the Gaming Practice Group in the Las Vegas office of the law firm, Lewis Roca Rothgerber LLP. His practice emphasis is on Internet gaming, sweepstakes, contests, restricted and nonrestricted gaming locations, and pari-mutuel wagering. He may be reached at KRutledge@LRRLaw.com.