

CYBERSECURITY AND DATA PRIVACY INFORMATION MEMO

JUNE 21, 2021

Website Terms of Use Agreement and Privacy Policy

Booming internet usage means that virtually every company has a website and many companies use their website to enhance the user experience and collect information about their users. As a result, company websites have terms of use and privacy policies that were developed to govern the interaction between the user and the company through its website.

Many companies, however, developed their website's terms of use and privacy policy when their websites were last substantially revised, and no one has paid attention to them since. Of more concern, some companies "cut and pasted" terms of use and privacy policies from other websites or used template forms available on the internet. While these may be a good start, they may miss some key provisions that should be included to protect your company and comply with the law.

This article reviews what needs to be included in terms of use agreements and privacy policies for company websites so that you can determine whether your company needs to review and update any of the provisions in them to better protect your company.

Terms of Use Agreements

These provisions are typically included in a hyperlink at the bottom of a webpage. They can also be named terms of service, terms and conditions, conditions of use or similar phrases. The first rule about these provisions is that they should be easy to read and understand. The provisions are intended to be a legal agreement binding on the website user which establish the terms a user must abide by to use the website.

Terms of use provisions generally include:

- Agreement to use the website only for lawful purposes (prohibits use of malware or other software that interferes with the content or use of the website);
- Disclaimer that the information on the site is for general information purposes and there is no warranty regarding the accuracy, completeness or usefulness of the information. The disclaimer should extend to third-party content if used on website;
- Acknowledgement that website content is owned by the company and is protected by copyright, trademark and other intellectual property laws, and the material cannot be reproduced or modified;
- If the website contains message boards, chat rooms or other interactive features, terms governing user-generated content so that user-posted material does not violate laws or company standards;
- An explanation of what information the company may collect from its website users and a link to the company's privacy policy (more on this later in this article);
- Notice that the terms of use may be revised and updated from time to time and that all changes are effective immediately upon posting;
- Email address for feedback or comments relating to the website; and

- Traditional contract provisions such as disclaimer of warranties, limitations on liability, governing law and indemnification.

Note that the terms of use agreement for your website should be tailored to fit your website, its functionality and your company. Terms of use are important if accounts can be created on your company's website because they set the rules about how the account system operates. Moreover, if there are links to social media features, specific concerns about copyright infringement (especially if there is user-generated content), concerns about collecting personal information of children using a site or industry-specific regulations (e.g. banking and financial services), there may be additional language that should be added to the terms of use agreement to protect your company.

“Browsewrap” vs. “clickwrap” agreements

A browsewrap terms of use agreement exists when the terms of use are referenced on the website's main page by a hyperlink to the complete provisions where there is a conspicuous notice that, by using the website, the user agrees to the terms of use. The website user must click on the hyperlink to see the terms that bind the user. Generally, courts have held that browsewrap agreements will be binding on the user when the user is encouraged by the design and content of the website to examine the terms available through the hyperlink.¹ However, courts have taken disparate views on whether a website is, in fact, appropriately designed to encourage the user to click on the terms of use hyperlink. If your company is using a browsewrap terms of use, a message should be displayed in a prominent position on the site's pages, notifying users that the website is governed by the terms of use and that users who do not agree to the terms must not access or use the site. This message should provide a link to the full terms of use and be located so that users can see the notice without having to scroll down the page.

A clickwrap terms of use agreement exists when a pop-up, or series of pop-ups, appear when users visits the website that informs them that they have to review and agree to the terms of use to use the site by clicking to indicate agreement. This is a clearer means to show user agreement to the terms of use and are more likely to be found enforceable by a court than browsewrap terms. E-commerce site where users are purchasing products or services and websites where social media is being uploaded or posted are advised to use clickwrap terms of use agreements to ensure enforceability of their terms.

Privacy Policies

Your privacy policy should disclose your practices when it comes to the collection, use, handling and sharing of data from your users. Privacy policies are now required by several federal, state and foreign laws, particularly if your company is collecting data to identify individuals (e.g. email address, name, mailing address, social media information, etc.). Any third-party advertising or analytics provider that your company engages to help optimize website use will require an acceptable privacy policy be posted by your company before it will integrate their services on your website.

It is a good practice to have a privacy policy even if your company is not collecting data that could identify individuals, if for no other purpose than to inform your users that you are not collecting any individually identifying data.

Your privacy policy should be easy for users to read and understand. It should be clearly and conspicuously accessible on the website. A link to the policy must be conspicuously placed wherever personal information is collected. It should truly reflect the company's actual business practices. The policy should not make any statements about the company's privacy practices that may turn out to be untrue.

¹ See, e.g. Berkson v. Gogo LLC, 97 F. Supp.3d 359 (EDNY 2015)

A privacy policy that meets the requirements of most data privacy laws should include the following provisions:

- A description of what kind of information you collect from users, why you collect it, how you use it, how long you store it and what information is shared with third parties;
- Disclosure on whether and how you use cookies or other tracking technology;
- Disclosure that the company may have to release collected user information in response to warrants, subpoenas or other legal process;
- How to request changes to, or a review of, any information of the user that is collected and stored;
- An opt-out procedure for users who do not want their information shared with third parties or used by the company;
- The method that will be used by the company to notify users of any changes to its privacy policy; and
- The policy should identify the date it was last revised.

The word “privacy” should be used in the title of the policy and any links to the policy.

Note that if your company sells advertising for its website that has click-through features or uses a vendor’s technology for analytics, those third-parties may be collecting user data as well and your privacy policy also needs to disclose the privacy practices of those third-parties.

Template privacy policy should not be used for most websites. Instead, a privacy policy should be carefully drafted that is informed by the company’s actual information collection and privacy practices.

Importantly, as technology evolves, so does the information that might be mined from company websites. Your company should periodically audit its compliance with its posted privacy policy and confirm that its practices, such as allowing users to opt-out of certain uses or disclosures (for example, to unsubscribe to a mailing list), are being followed. Failing to comply with what you have promised to do in your privacy policy exposes the company to potential liability.

As this article highlights, while provisions in terms of use agreements and privacy policies on company websites may look “boilerplate,” they are not. These must be tailored to the capabilities and functions of your website and to the specific information that is being collected and stored from user use.

If you have any questions about the information presented in this memo, please contact [Gail Norris](#), any [attorney](#) in the [Cybersecurity and Data Privacy](#) practice or the Bond attorney with whom you are regularly in contact.

