PREPARED BY

GalkinLaw

internet law · new media law · technology law

Guide to Preparing Website and App Privacy Policies

GOT QUESTIONS ABOUT WEBSITE AND APP PRIVACY POLICIES?

CONTACT US FOR A FREE CONSULTATION AT

WWW.GALKINLAW.COM | INQUIRIES@GALKINLAW.COM | (410) 484-2500

GUIDE TO PREPARING WEBSITE AND APP PRIVACY POLICIES

INTRODUCTION

Privacy is a critical issue on the Internet. Users have become accustomed to seeing Privacy Policies posted on websites and in apps. While for most websites and apps operating in the U.S. a Privacy Policy is not legally required, it would certainly be viewed as a bad practice not to have a Privacy Policy, and many cyber protection services will flag such websites.

Currently, the only state that actually requires websites and apps to have a Privacy Policy is California. However, since almost every website or app will have users resident in California, it is therefore the rare "local" website or app that would not need comply with the California law on this issue.

1. BACKGROUND AND APPROACH

Privacy Policies primarily regulate how a website or app collects personal information from its users and how such information will be used and transferred. In the U.S., the Federal Trade Commission (FTC) is primarily responsible for the enforcement of privacy commitments.

The FTC considers statements in a Privacy Policy to be promises made by the website or app to the users. Therefore, when drafting Privacy Policies, great care must be made to verify the accuracy of all claims and obligations contained in the Privacy Policy. The Privacy Policy needs to accurately reflect the collection, storage, use and dissemination polices applicable to the information. Failure to keep these promises may amount to an unfair or deceptive trade practice actionable under the FTC Act. Additionally, Privacy Policies need to be prepared in a flexible manner that anticipates future needs of website or app and their owners.

It is often tempting to grab a Privacy Policy from another website or app and model it for a new website's or app's purposes. However, "getting it right" the first time is critical for a Privacy Policy, not only because of potential liability, but also because later changes to the Privacy Policy may seek to correct earlier mistakes or misunderstandings but may not apply to earlier collected information. This could have several significant negative results, like obstructing the implementation of new marketing plans, requiring costly administration to distinguish between information that needs to be handled in accordance with different policies and placing a cloud on potential liability and ownership in information that will scare off potential investors and purchasers.

It is important to note that privacy obligations are broader than mere compliance with the Privacy Policy. For instance, some states have implemented laws that impose obligations as to how personal information is maintained and almost all have laws governing activities that must be undertaken if personal information is breached. Financial information may be governed by the Gramm-Leach-Bliley Act (GLBA), medical information by Health Insurance Portability and Accountability Act of 1996 (HIPAA), and information about children under the age of 13 by the Children's Online Privacy Protection Act (COPPA). Also, where users are located in other countries or where personal information is being transferred from or to other countries, then

the privacy laws of such other countries may also be binding upon a U.S. based website or app.

2. SPECIFIC TERMS

While there are various provisions that may be relevant, following are some of the main provisions and issues that need to be considered when preparing Privacy Polices.

A. WHAT INFORMATION IS BEING COLLECTED

Privacy Policies need to specify the type of information that will be collected. It is best to be broad in the description. However, it is not a good privacy practice to collect more information than is reasonably necessary for the purposes of the website or app. Descriptions of information collected would usually include all of the typical personal contact, identity and preference information, but should also include the non-obvious information like IP address, browser type, host operating system, etc. that is automatically collected. When geo-location information is being collected from a mobile device or information is collected via the microphone or camera, then specific express consent should be obtained when such features are activated. Under the Children's Online Privacy Protection Act (COPPA), parental permission is required to collect personal information from children under the age of 13. There are narrow exceptions to this requirement, and the method of verifying parental consent needs to be strictly complied with.

While the primary consideration is personally-identifiable information, the use and transfer of non-personally-identifiable information that is collected should also be disclosed.

B. HOW USER INFORMATION BEING COLLECTED

Personally-identifiable information and non-personally-identifiable information can be collected by a variety of means, through registration forms, user postings, surveys, communications with the website or app, by means of cookies and web beacons, etc. These methods should be clearly stated.

C. HOW INFORMATION IS BEING USED

Information may be used for a variety of purposes, such as to personalize content presented to users, to serve advertising and deliver other information, market research purposes, carry out agreements entered into between the website and the users, and to notify users about changes and features of the website. These uses should be clearly stated.

D. THIRD PARTIES THAT MAY BE COLLECTING OR RECEIVING INFORMATION

Third parties that will be receiving personal information of users should be clearly stated. Often there are third party service providers that will be receiving personal information on behalf of the website or app. Such service providers may include credit card transaction processors, communication platform providers, and hosting services providers.

Information may also be transferred to third parties for marketing purposes. If there are legal proceedings involving the website or app, the website would want express acknowledgement from the users that the website may cooperate with such proceedings, which may include a transfer of personal information to legal authorities. Additionally, it is critical to allow transfer of the information to an entity that may acquire ownership in the website at a future date.

Advertising served by third parties automatically receives IP addresses and such third parties may also use cookies, JavaScript, web beacons and other technologies to measure the effectiveness of their ads, to personalize advertising content, to compile anonymous statistics and otherwise monitor the effectiveness of their campaigns. Users should be notified in the Privacy Policy of these possibilities. It is also beneficial to highlight to users that there may be links in the website or app to third party websites or apps and that the privacy policies of such third party websites will govern the collection and use of their information.

E. SECURITY USED TO PROTECT INFORMATION

Websites and apps are not generally required to state the type of security that will be in place to protect the information from unauthorized access. However, many users what to see this. Once security procedures are stated, failure to comply with such procedures could subject the website to action by the FTC. Therefore, it is important not to overstate the actual security that will be in place. It is also important to clearly state the limitation of any security system. No system is absolutely secure from unauthorized access from hackers.

F. COMPLIANCE WITH U.S. AND NON-U.S. LAWS

The Privacy Policy should contain provisions so that marketing communications do not violate the CAN-SPAM Act. California in particular has implemented privacy laws that may impose additional requirements on a U.S. website and app that collects personal information from California residents. Additionally, if user information will be collected from individuals located in non-U.S. jurisdictions, then the Privacy Policy may also need to contain provisions that comply with European Union Privacy Directive requirements or the requirements of other jurisdictions.