Practical Guidance

Website Policy and Agreements

A Practical Guidance® Practice Note by
Kavon Adli and Jason Civalleri, The Internet Law Group

Kavon Adli
The Internet Law Group

Jason Civalleri
The Internet Law Group

This practice note provides guidance on drafting policies and agreements that are commonly posted on websites. Such policies may address and/or involve, among other things, privacy issues, website terms and conditions, sale terms and provisions, permitted use(s) of and guidelines for the website, delivery and return policies, trademark and copyright guidelines and policies, legal agreements, and disclaimers.

For additional information, see Business Website Contractual Issues and Privacy Policies: Drafting a Policy. For form website policies, see Website Terms of Use, Website Terms and Conditions of Use (Website Provides Information and Services), Website Terms and Conditions of Use (Website Provides Information for a Fee), Acceptable Use Policy, and Subscriber Agreement and Terms of Use for Website with User-Generated Material.

Effectiveness of Agreements and Policies Online

The enforceability of any of the agreements, documents, or policies described below hinges upon two key factors: (1) prompt, effective notice to a user of their existence through conspicuous placement and unambiguous language; and (2) user assent, either explicitly or by inference, based upon the user's conduct. Therefore, in order to maximize the likelihood of enforcement of a particular agreement, document, or policy, it should:

- Provide clear and conspicuous notice to users of all of its terms
- Require users to scroll to the bottom and type their name in a signature box, click "I Agree," or otherwise expressly manifest assent thereto in an unambiguous manner before engaging in conduct subject to its terms
- Prohibit any use or access to covered conduct prior to the requisite express manifestation of assent
- Require reconfirmation of such express manifestation of assent on a periodic basis
- Ensure that all of the applicable terms are enforceable according to contract law in general (including good faith and fair dealing, consideration, adhesion, unconscionability, etc.)

Website operators may have concerns or preferences regarding displaying and documenting interactions that do not align with legal effectiveness. Counsel should advise clients as to the most effective methods for coverage, while being mindful of business interests, legal effectiveness, and website ease of use.

Generally, documents should be displayed in a friendly and easy-to-read format to ensure users understand their provisions. Counsel should consider the expected reading level of their intended audiences; for example, portions of documents drafted for a child's website should be written in language appropriate for a younger audience. "Legalese" and other highly technical language is discouraged, particularly in documents intended to bind consumers or non-sophisticated users.

While Terms and Conditions (T&Cs) and privacy policies should be separately presented to users of most websites, other documents are commonly nested into these primary documents to reduce the apparent legal footprint. Excessive unwieldiness, however, may hide important provisions or be confusing. Depending on their complexity and appropriateness to stand on their own, these documents may also be incorporated into the primary documents by reference to another page (preferably via hyperlink).

The legal documents, policies, agreements, and notices described below can be displayed through either browsewrap or clickwrap. Browsewrap requires the user to browse the website in order to find the documents (which are usually located in links toward the bottom of the page), and clickwrap involves the user clicking "I Agree" in order to affirmatively indicate its acceptance of the documents. Clickwrap is clearly a stronger legal method of agreement, providing a much higher certainty of protection than browsewrap as browsewrap merely presumes that the user has agreed to the terms in the applicable documents. Maximum legal coverage may involve document presentation as a pop-up when a user first accesses a page or begins the process of entering a transaction where such document applies. This ensures that the agreements have a fair opportunity to be seen and that the user has actual notice of their existence, content, and applicability. Legal effectiveness may require users to expressly and unambiguously manifest assent to an agreement or policy (possibly on a periodic basis) such as requiring users to scroll to the bottom of an applicable document and type "I Agree" before accessing the relevant pages or completing transactions. In cases where a company is not comfortable providing (or continuing to provide) content, goods, or services to users who do not agree to their terms, users may be prohibited from accessing some or all of the company's content, goods, or services until after expressing manifestation of assent.

For further guidance on considerations for entering effective online contracts, see Electronic Contracts — Online Contracting.

Privacy Policies

A website privacy policy notifies users about the website operator's procedures with respect to its collection, use, disclosure, sharing, storage, and sometimes deletion of personal information (including names, online identifiers, addresses, phone numbers, credit card information, age, contacts, photos, calendar, health information, genetic or biometric information, and financial information). This incredibly important document is required for most websites' compliance with federal and state regulations, and is essential in creating and preserving the trust of a website owner's users. Privacy is a major concern and enforcement priority for the Federal Trade Commission (FTC), particularly when it comes to protecting the privacy of children. When information falls into the wrong hands, problems such as harassment, stalking, and identity theft, to name a few, inevitably ensue. Strong precautionary measures must be taken to protect consumers and comply with applicable federal and state privacy and security laws, including the maintenance of an easily accessible privacy policy detailing all collection and use of personal information. The privacy policy should be seen as reflecting a company's actual procedures and policies in place regarding personal information (as opposed to a standard document purporting to satisfy privacy law requirements), which may need to be crystalized before or in tandem with authoring an effective privacy policy.

The following key provisions should be included in any effective privacy policy:

- Identify what data will be collected by the website and third-party providers. This falls into three main categories:
  - **User-submitted information.** Such information is usually provided during the registration process or during use of the website.
  - **Information collected automatically.** Some examples are IP addresses, geolocation, operating system, mobile device identification, browser, advertisements clicked on by the user, and amount of time spent on the website.
  - **Cookies.** A website operator must disclose any use of cookies, web beacons, or other tools on its users' computers to collect and track their movements online.
- Recognize what options are available to prevent such collection (and its dissemination to third parties), including the potential provision of a "Do Not Track" feature to prevent tracking by advertising networks and other third parties.
- Explain how exactly the data is used and with whom it will be shared (i.e., service providers, analytics companies,

advertisers, law enforcement). This should also cover in what form the information is shared (i.e., in an aggregated and anonymized form or with all personally identifying elements attached).

- Describe how the data will be stored and protected (i.e., a general description of which security measures are in place).
- Include any additional information required by applicable state and industry laws and guidelines, such as (1) the Health Insurance Portability and Accountability Act (HIPAA), 104 P.L. 191, which is applicable to healthcare-related activities; (2) the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., which is applicable to the financial services industry; (3) the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., which is applicable to data broker activity; and (4) the Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6501 et seq., which is applicable to child-directed content (websites that are not intended for children should include a statement to this effect).
- Articulate how a user can see what data is being held about him or her, and what he or she can do to change, delete, and/or update it.
- Describe the company's policies related to complying with a court order, subpoena, search warrant, law, or regulation that may require disclosure of users' personal information.
- Include dispute resolution information.
- Note the effective date of the policy, including any and all updates.
- Include contact information (i.e., where notices should be sent).

With respect to e-commerce websites, the applicable privacy policy must also include:

- Security measures taken to protect the financial information provided by the user (i.e., credit card information used for purchases, etc.), which should always be encrypted as a protective measure
- Information respecting when and under what exact circumstances a user's financial information will be released to financial regulatory bodies for anti-fraud and/or anti–money laundering purposes

Federal and State Privacy Policy Law

While no generally applicable federal privacy policy law exists, the policies are usually enforced by the FTC under its authority granted by Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits unfair or deceptive marketing practices. Additionally, private parties can enforce their terms by filing lawsuits directly against the website operator issuing the policy, although this can sometimes be thwarted by a company's use of arbitration clauses and/or other provisions of its terms of service. The federal laws set forth above (i.e., HIPAA, COPPA, etc.) also serve to govern and enforce the use and terms of company privacy policies.

Many states have also enacted their own privacy policy regulations. California has enacted several such regulations. The California Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code § 22575, requires any commercial websites or online services that collect personal information related to California residents through a website to conspicuously post a privacy policy on the site. Other states, including Nebraska and Pennsylvania, have enacted laws that treat misleading statements in privacy policies as deceptive or fraudulent business practices as well.

California Privacy Regime

California also passed the nation's first comprehensive consumer privacy regime in its California Consumer Privacy Act of 2018 (CCPA). Cal. Civ. Code § 1798.100 et seq. CCPA requires additional practices related to Californians' personal information (and corresponding notices in the privacy policies) by any for-profit company that does business in California and (subject to certain exceptions) meets any of the following thresholds: (1) realizes at least $25 million in gross annual revenue; (2) buys, sells, or receives personal information related to 50,000 or more California residents, households, or devices; or (3) derives at least 50% of annual gross revenue from the selling of California residents' personal information. CCPA requires that companies that meet this threshold take certain steps toward protecting users' personal information and have certain procedures in place to allow users to exercise certain statutory data rights, all of which must be reflected in a CCPA-compliant privacy policy. For further guidance on CCPA, see CCPA Regulations Compliance: Notice Requirements. In 2020, California passed the California Privacy Rights Act (CPRA) by ballot initiative, which amends the CCPA and includes additional privacy protections for consumers. Among other modifications, the CPRA adjusts the CCPA's applicability to for-profit businesses that do business in California and (subject to certain exceptions) meet any of the following thresholds: (1) realizes at least $25 million in gross annual revenue; (2) buys, sells, or receives personal information related to 100,000 or more California residents or households; or (3) derives at least 50% of annual revenue from the selling or sharing of California residents' personal information. The CPRA goes into effect on January 1, 2023, with a "look-back" provision allowing enforcement regarding companies' practices after January 1, 2022.

Virginia and Colorado Privacy Regimes

Virginia and Colorado are the first states to follow California's lead in passing state-level comprehensive consumer privacy regimes. Virginia recently enacted its Consumer Data Privacy Act of 2021 (CDPA), which imposes obligations on entities conducting business in Virginia or selling goods or services targeted toward Virginia residents that either (1) control or process personal information related to 100,000 Virginia residents, or (2) control or process personal information related to at least 25,000 Virginia residents and generate at least 50% of gross revenue from the sale of personal information. Similarly, Colorado's recently enacted Privacy Act (CPA) imposes obligations on companies that produce or deliver products or services that are intentionally marketed to Colorado residents, and either (1) control or process personal data pertaining to at least 100,000 Colorado consumers per year, or (2) derive revenue or receive discounts from other vendors for the sale of personal data and process or control the personal data pertaining to at least 25,000 Colorado consumers. Like the CCPA and CPRA, the CDPA and CPA place certain privacy practice obligations on covered entities that must be reflected in their privacy policies. While the requirements under CCPA, CPRA, CDPA, CPA vary in some ways, counsel advising companies whose websites attract users in California, Virginia, or Colorado should consider the ramifications and requirements under the CCPA (as modified by the CPRA), CDPA, and CPA when drafting privacy policies.

Nevada Privacy Requirements

Counsel should also be aware of requirements placed on certain website operators in Nevada, which, although less comprehensive than the CCPA, CPRA, CDPA, or CPA, may apply to their clients' privacy policies. Nevada passed the Nevada Privacy of Information Collected on the Internet from Consumers Act of 2017 (Nevada Privacy Law) that requires a privacy policy be posted by persons or companies that (subject to certain exceptions) (1) own or operate a website or online service for commercial purposes; (2) collect and maintain certain covered information from consumers who reside in Nevada and use or visit the internet website or online service; and (3) purposefully direct their activities toward Nevada, consummate some transaction with Nevada or a resident of Nevada, purposefully avail themselves of the privilege of conducting activities in Nevada, or otherwise engage in any activity that has a sufficient nexus with Nevada. The Nevada Senate amended the Nevada Privacy Law in 2019 in SB 220, requiring covered website operators to disclose in their privacy policies how Nevada consumers may exercise a right to opt out of the sale of their personal information. The Nevada Senate again amended the Nevada Privacy Law in 2021 in SB 260, which, among other modifications, clarified requirements for covered website operators who perform services as, or interact with, "data brokers."

As states grapple with determining how to protect their residents' privacy rights, we can expect more states to follow California's lead in enacting new laws that may impact privacy policy content. Beyond the laws mentioned in this note, counsel should frequently review and consider how states are addressing this issue when drafting privacy policies.

For further guidance on privacy issues, see Electronic Communications Privacy Act (ECPA): Key Issues, General Data Protection Regulation (GDPR), Mobile Application Privacy Compliance, Privacy Policies: Drafting a Policy, COPPA Privacy Policy, Mobile Application Privacy Policy (General); Online Privacy Notice (Product or Services Sales Website), and Social Media Privacy Policy (Short Form).

Terms and Conditions

T&Cs, also known as Terms of Use or Terms of Service are legally binding agreements that set forth website operators' rules with respect to how their websites may or may not be used. T&Cs are often considered the central agreement guiding the relationship between website users and administrators, and often serve as the primary vehicle through which most other documents, agreements, and policies can affect such a relationship. T&Cs, while subject to change, should always incorporate the following information:

- A conspicuous statement that notifies the user that the T&Cs is a contract, and that users agree to the contract by visiting the website
- A notice that the T&Cs may be modified from time to time
- Prohibitions of misuse of the website or related services
- Account suspension and/or termination procedures in the event of misconduct
- Disclaimers, warranties, and limitations of liability
- Consent language for collecting personal information
- How a user's intellectual property is protected and any applicable takedown notice procedures

T&Cs may also incorporate several of the policies, provisions, and agreements below. Effective T&Cs should identify any other policies, documents, or agreements that are incorporated into the agreement (ideally via hyperlink, if appropriate), including language acknowledging a user's receipt of those documents and agreement to be bound by their terms.

For additional information on T&Cs, see Website Terms of Use, Website Terms and Conditions of Use (Website Provides Information and Services), Website Terms and Conditions of Use (Website Provides Information for a Fee), and Website Terms of Use (Copyrighted Web Content).

Terms of Sale

With respect to e-commerce websites, additional information or provisions regarding transactions involving other goods or services offered on the website (Terms of Sale) should also be addressed. Terms of Sale are commonly either provided as a standalone document on a website or embedded directly into the website's T&Cs, as is appropriate for the particular website and the particular documents. If and as applicable, an effective Terms of Sale should include:

- Payment details for purchases
- Disclaimers and warranties relating to the goods and/or services offered
- Return and refund policy information, including, at a minimum: when, under what circumstances, and within what time frame returns are permitted; where returned items are to be sent; and which party is responsible for the associated shipping costs (Return and refund policy information is sometimes in a separate agreement. For more information, see the Return and Refund Policies section below.)
- Installment payment information
- Late payment penalties and interest information
- Instruction on how to enter the company's internal dispute resolution or customer support systems before seeking external adjudication of any complaints or disputes

Further, if a website's goods or services are offered on a recurring or subscription-based billing (Negative Option) model, such transactions may be subject to additional regulation under Section 5 of the FTC Act, 15 U.S.C. § 45, the Restore Online Shoppers' Confidence Act (ROSCA), 15 U.S.C. § 8401 et seq., the Trade Regulation Rule Concerning Use of Pre-notification Negative Option Plans (Negative Option Rule), 16 C.F.R. § 425, or certain state laws. Required notices and terms guiding a Negative Option arrangement may be at least partially addressed in a Terms of Sale. For further guidance on Negative Option model considerations, see Negative Option Marketing.

Shipping and Delivery Policies

This document sets forth all of a website operator's policies and procedures with respect to the shipping and delivery of goods to its customers. Shipping and delivery policies (if and as applicable) should be incorporated into the Terms of Sale, either directly or by reference (preferably via hyperlink). Well-drafted shipping and delivery policies should contain the following information:

- **Delivery dates and shipping fees.** Most policies provide customers with several options at various price points for delivery (i.e., overnight, 5–7 business days, 10–12 business days, etc.). Shipping fees and applicable taxes, including international fees, are set forth alongside these options. Free shipping is usually offered for purchases equal to or above a certain dollar amount as an incentive to spend. Additional information regarding back orders, curbside delivery, tracking numbers, and partial deliveries should be included as well. Companies usually reimburse their customers for shipping delays to the extent that payment was made for expedited delivery, although this information is rarely in the applicable shipping and delivery policy.
- **The names of the shipping carrier(s) used.** Commonly used shipping carriers are UPS, FedEx, DHL, and USPS. Customers should also be informed as to whether or not they can receive shipments at a P.O. Box.
- **Assurances of refunds or replacements in the event that the goods purchased are either not delivered or damaged upon receipt.** These assurances are necessary to provide proper customer service and maintain the integrity of a business. They should be made expressly subject to specific customer notification procedures, however, including (1) prompt notification to the company specifying in reasonable detail the issue(s) and (2) the timely provision of additional information as necessary (i.e., a requirement to provide photographs of damaged goods). Companies almost always have insurance covering this issue.
- **Order modification and cancellation terms.** Most bona fide companies provide their customers with the right to change and/or cancel an order free of charge if any such change or cancellation is made prior to delivery efforts having commenced. A shipping and delivery policy may also incorporate a company's return policy, unless such return policy is provided as a separate document. See the Return and Refund Policies section below.

- **Information regarding fraud prevention activities.** Companies should, and usually do, verify billing and shipping addresses in order to protect against identity theft and provide users with a safe shopping environment. A shipping and delivery policy should incorporate language informing the website operator's customers that during this verification process a customer and/or a customer's credit card company or issuing bank may be contacted. Further, the policy should disclose that to the extent fraud is detected (1) the order will be cancelled, (2) the customer will be contacted, and (3) local law enforcement will be informed.

The enforceability of a shipping and delivery policy by a website operator hinges upon the same notice and assent principles as in the Effectiveness of Agreements and Policies Online section above. This includes, without limitation, ensuring that users unambiguously manifest assent prior to making a purchase.

Return and Refund Policies

An e-commerce business must always inform its customers about its return and refund policies, which may be accomplished by posting its policies related to returns and refunds. This document (if and as applicable) should be incorporated into the Terms of Sale, either directly or by reference (preferably via hyperlink). Effective return and refund policies should clearly and conspicuously provide information to accomplish the following:

- Clarify whether returns and/or refunds are offered on physical goods, services, and/or digital products or services
- Pinpoint what goods and/or services are not returnable (i.e., custom and specially ordered items, items on sale, or purchased with a discount or coupon)
- Mention how much time a customer has to make a return and receive a refund or store credit, if applicable
- Clarify who is responsible for shipping costs
- Provide restocking fee information, if applicable
- Describe the procedure for effectively requesting a return or refund, including any necessary or helpful documentation to be submitted (i.e., a receipt, purchase or invoice number, photos of defective or damaged merchandise)

Most e-commerce companies permit returns and refunds voluntarily as proper business practice. They are not, however, legally required to accept returns unless the goods sold are defective and/or if the retailer otherwise breaches the applicable sales agreement. The FTC provides a "Cooling Off Rule," 16 C.F.R. § 429.0 et seq., which gives customers a three-day window to cancel any purchases equal to or greater than $25.00. Additionally, most states maintain laws respecting refunds, including (1) a requirement that refund policies be prominently displayed at the point of purchase in order to be valid, and (2) the right to rescind club memberships (i.e., gyms) or other specialty sales contracts within a specified number of days. If a company does not permit returns or refunds, it should clearly disclose in its Terms of Sale.

Community Guidelines

Community guidelines are a website operator's "rules of play," as they inform users what is and is not acceptable in their online communities. They are used primarily by social media companies or online multiplayer gaming services. Community guidelines encourage users to treat each other with respect and act appropriately at all times. They are generally written in a friendly, casual tone. Their primary focus, however, is on what a user should *not* do. The list most commonly includes the following actions that the user should not engage in:

- Violate the intellectual property rights of any person or entity
- Upload or send spam or malware
- Engage in activity considered immoral, sexually explicit, or patently offensive
- Engage in any illegal activity
- Harass and/or stalk someone
- Engage in hate speech or other polarizing and incendiary conversation
- Impersonate others and/or create fake accounts
- Promote or glorify self-harm or violence
- Engage in username/URL squatting
- Post deceptive or fraudulent links
- Engage in unauthorized or unlicensed commercial activity (i.e., an unauthorized sweepstakes)
- Fail to moderate content based upon probable viewership (i.e., children)
- Engage in any other behavior which is reasonably likely to cause conflict or trouble
- Attempt to harm or exploit minors or otherwise expose them to indecent or harmful content

Ideally, community guidelines should set forth information about the actions that the website owner will take in the event that a member or user is violating any rules, which may include one or more of the following (if and as applicable): (1)

issue verbal or written warnings, (2) remove the questionable content. (3) suspend or terminate the user's account, (4) report any illegal activities to the local authorities, and/or (5) pursue other legal action or remedies. As with other company policies, discipline should be meted out fairly and consistently among community members.

Community guidelines (if and as applicable) should be incorporated into the T&Cs, either directly or by reference (preferably via hyperlink). Depending on the circumstance, they may be suitably provided on a clickwrap or a less effective browsewrap basis when users are required to create accounts or otherwise attempt to interact with a website's community.

Trademark Usage Guidelines

Trademarks are specific words, pictures, and/or other symbols that are used by businesses to mark the identity of their goods and services. Trademarks that are used to identify services are usually called "service marks." Only the trademark owners are permitted to use their personal marks; their right to this form of intellectual property is exclusive. Trademark usage guidelines serve to delineate a user's rights with respect to a company's trademarks. Well-written guidelines should always include the following information:

- A complete and regularly updated list of the company's trademarks (both registered and unregistered)
- A reference to the applicability of the guidelines, superseded only by a fully executed license agreement between licensor/company and licensee/user
- A statement to the effect that any trademark use is subject to the company's prior written authorization in each instance (granted in its sole discretion), as well as the relevant guidelines
- Contact information for requesting permissions and licenses
- An acknowledgment that trademark ownership is and shall remain at all times with the licensor/company
- A statement to the effect that the right to use a company's trademark, if granted, is nontransferable, non-exclusive, and revocable at any time, all subject to the terms of any applicable license agreement and the guidelines
- A list of rules and restrictions with respect to authorized trademark usage, including:
    - Do not bring harm or disrepute to the company and/or the goodwill of a trademark
    - Do not use a trademark in metatags, search fields, hidden text, or any other form that may divert or confuse users, unless prior written consent is first obtained
    - Do not make references to the company or its affiliates, brands, products, or services that are unfair, untruthful, derogatory, or misleading in any way
    - Do not use a trademark without providing the requisite acknowledgment of company's ownership in and to the mark in the form and manner specified by company
    - Do not modify or edit a trademark in any way
    - Do not incorporate or combine a trademark with any other product or service mark, logo, or company name, or with any other words or images of any kind
    - Do not adopt marks or logos that are confusingly similar to a company's trademark
    - Do not use a trademark in a manner that could reasonably suggest a sponsorship or endorsement by the company, or confuse the company's brands with any other brands
    - Do not associate a company's trademarks with indecency, illegality, vulgarity, pornography, racism, prejudice, obscenity, or any other patently offensive or incendiary content or information of any kind
    - Do not engage in cybersquatting (i.e., incorporating a company's trademark into a separate entity's domain name, in whole or in part)

Trademark infringement is enforceable under (1) the Lanham Act of 1946, 15 U.S.C. § 1051 et seq., as amended; and (2) the Trademark Counterfeiting Act of 1984, 15 U.S.C. § 1116(d).

Copyright Notices/Policies

A copyright is the exclusive legal right given to the owner (usually, the creator) of unique literary, artistic, or musical material to produce, reproduce, perform, record, display, broadcast, or make derivative works of any such material, or to authorize or assign other parties the right to do the same. 17 U.S.C. § 106. A copyright policy provides users with notification that the contents of a company's website are fully protected by U.S. copyright law. While not legally required in order to protect the intellectual property it covers, a well-written policy serves to inform and remind users what the applicable laws are with respect to the materials and information contained on a website.

Copyright policies should incorporate the following information:

- A definition of copyright and brief summary of copyright law
- A list of permissible activities, which most commonly includes the following:
  - The right to view and store content for personal use
  - The right to print single copies of articles on paper for personal use
  - The right to share links to information using the sharing tools provided by the applicable website
  - A limited right to share portions of articles or other information in order to permit "fair use" (a U.S. legal doctrine codified in 17 U.S.C. § 107 that allows for a limited use of copyrighted material without permission for educational, journalistic, political, or artistic purposes only) subject to certain obligations, such as proper source credit (using a textual link only) and limitations on use/purpose (i.e., no commercial use, no endorsement activity, and no editing or alterations)
- A list of prohibited activities, which most commonly includes the following:
  - Reproduction or distribution of materials or information contained on a website for commercial use
  - Improper or unauthorized retention of intellectual property
  - Any reproduction or distribution not properly considered to be fair use
  - Use of materials without any and all required third-party licenses (a situation commonly seen when a website operator has received permission to republish a photograph from the owner, yet the user has not)
  - Restricting the authorized reposting of content to limited user groups (i.e., as opposed to making such content free of charge and accessible to anyone with or without an account)
  - Making and distributing copies of materials, articles, or other information for any reason without permission
  - Editing or altering the content in any manner
  - Making use of any reproduced content or information in violation of any of the applicable website's T&Cs or other policies
- Digital Millennium Copyright Act (DMCA) enforcement information and procedures:
  - **DMCA.** The DMCA of 1998, 17 U.S.C. § 1201 et seq., is a federal copyright law enacted primarily to curb the piracy of digital media. The DMCA makes it illegal to host, share, or download copyrighted works (including music, movies, books, software, videos, photos, etc.) without the owner's permission. Title II of the DMCA, 17 U.S.C. § 512, also known as the "safe harbor" provision, effectively created a conditional safe harbor for online service providers (OSPs) against copyright infringement liability. The safe harbor states that OSPs are not liable for the transmission of materials that may infringe a copyright, provided, however, that they (1) provide their users with information about their policies with respect to copyright infringement, and (2) block access to or remove the allegedly infringing material promptly upon receipt of a confirmed notice from the copyright holder (i.e., a "DMCA Takedown Notice"). Unlike other copyright infringement remedies, a copyright does not have to be registered in order to take advantage of this safe harbor.
  - **Safe Harbor and Website Operators.** The safe harbor provisions also provide valuable protection to website operators, who must provide the following information in their copyright policy (or in the terms of service if no separate copyright policy exists) in order to take advantage of them:
    - Designation of an agent (registered with the U.S. Copyright Office) with up-to-date contact information to receive copyright infringement notices
    - Provision of information regarding procedures to be taken in the event of an alleged infringement by a user, including suspension or termination of a repeat offender's account and/or access to the website in question
    - Prompt compliance with DMCA Takedown Notices, including (1) removal of the infringing material, (2) notification to the user or subscriber that the infringing material has been taken down, (3) notification to the copyright holder if a proper counter-notice is provided by the user or subscriber, and (4) restoration of the removed material if and when the proper counter-notice is provided, and the copyright holder does not file a lawsuit claiming infringement within 10 days thereafter

Legal Disclaimers

A legal disclaimer is issued by a website operator in order to limit its obligations and/or exposure to liability and damages. They usually vary from company to company depending on the products, services, and industry in general, and sometimes reference established statutory disclaimers (e.g., the DMCA safe harbor provision).

Some of the most common and effective disclaimers include the following:

- The "as is" disclaimer (i.e., that a company, while having made all commercially practicable attempts to ensure the accuracy and reliability of the information it has provided online, has provided such information "as is" and therefore without warranty of any kind, and as such, is not responsible or liable for the accuracy, content, completeness, legality, or reliability of the information)
- A disclaimer stating that a company cannot and will not guarantee that its website is free from computer viruses or other similar destructive properties
- A disclaimer stating that warranties, promises, or representations of any kind, expressed or implied, are *not* given as to the nature, standard, suitability, or accuracy of information provided online
- A disclaimer stating that the company is not liable for any loss, cost, or damage of any kind, including indirect or consequential, whether arising in contract, tort, or otherwise, which may arise as a result of a customer's use of, or inability to use, the company's website or the information contained therein (including any third-party website to which company's website is linked)
- A disclaimer of responsibility regarding the collection, storage, or use of personal data by any third-party entity
- A disclaimer of responsibility regarding the accuracy of third-party advertisements

Additionally, industry-specific disclaimers are commonly included. For example, most legal websites set forth a "no attorney-client privilege" disclaimer, informing potential clients that an attorney-client relationship is not established until the firm is formally engaged, and, therefore, potential clients should not rely upon the transmission of an email message to an attorney through a firm's website to establish any such relationship. E-commerce websites should also consider including disclaimers related to their products and services (if and as applicable), such as a disclaimer of any express or implied warranties (such as the implied warranties of merchantability or fitness).

Disclaimers must be clear and conspicuous to be enforceable so users have actual or constructive knowledge of their existence. However, a disclaimer may not be enforced if it is superseded by federal or state statute or if the clause is unconscionable.

Linking Policies/Agreements

A linking agreement is a document that incorporates a website operator's policies with respect to (1) third-party links on its own website, and (2) the placement of links (directing traffic to the site owner's website and/or online advertisements) on third-party websites. A linking policy can be included in a separate agreement or incorporated in another legal notice. Major search engines place a high value on links, as pages with a greater number of links tend to rank higher in search results. Higher rankings translate to more traffic, and therefore, website owners look to attract links to their sites as much as commercially practicable. Certain links, however, can give rise to legal and other issues, and as such, linking policies are designed to address potential problems before they arise by setting forth rules and processes in advance. Linking policies are sometimes referred to as "hyperlink policies," "web linking policies," or "linking statements."

The following provisions should be incorporated in a website owner's linking policy:

- The right to create a link is non-exclusive and can be terminated by the website owner at any time with very short notice (usually one day or immediately in the event of a breach of the linking terms).
- The third party creating a link must affirmatively accept the terms of the owner's linking policy in advance.
- The third party may not create frames around the owner's website or use other techniques (e.g., deep linking) that would alter the appearance/presentation of the site or display the website, in whole or in part, on another site.
- The third party may not use the website owner's logos, trademarks, service marks, or other proprietary images, brand names, icons, or other intellectual property without the prior written permission in each instance. All hyperlinks must be standard text-based links only (i.e., no images, etc., without such permission).
- The third party and its website must (1) be in compliance with all applicable laws, rules, and regulations at all times; (2) not engage in or display unethical, discriminatory, pornographic, violent, offensive, illegal, misleading, or indecent behavior, ideas, images, links, language, or dialogue or any kind; (3) not use political, cultural, religious, or other cultural symbols that may reasonably offend any particular group of people; (4) not disparage the owner's website or its brand, image, reputation, products, or services in any way; and (5) not infringe upon the intellectual property rights of any person or entity (including owner) at any time.
- The website owner shall not be responsible for any loss, damage, liability, or expense that may arise as a result of a third party's linking or other activities, and the third party should indemnify the owner for any such loss.

- The website owner shall not be responsible for any loss, damage, liability, or expense that may arise as a result of any user's involvement with or activities on any websites that are visited as a result of clicking on a third-party link on the website owner's site.
- Links should be only directed at the website's home page.
- Neither inbound nor outbound links shall be established in a manner to suggest any form of association, approval, or endorsement without prior express approval.
- All linked websites and their contents must conform with all of website owner's policies as set forth online or as additionally provided.

As with other website operator policies, linking policies are more easily enforced when posted in a clear and conspicuous manner. Enforcement activities include (1) disabling nonconforming links, (2) reporting illegal activity to local authorities, (3) issuing verbal or written warnings, and (4) seeking injunctive relief and/or monetary damages.

For further guidance, see Website Linking Permission Agreement (Long Form), Website Linking Permission Agreement (Short Form) and Linking and Other Special Issues Checklist.

Related Content

Practice Notes

Commercial Transactions

- Business Website Contractual Issues
- Electronic Communications Privacy Act (ECPA): Key Issues
- Mobile Application Privacy Compliance
- Privacy and Data Security Considerations When Negotiating or Reviewing a Transaction or Agreement
- Privacy Policies: Drafting a Policy
- Electronic Contracts
- E-Commerce Fundamentals
- E-Commerce Payment Mechanisms
- Internet of Things Key Legal Issues
- Social Media Sites and Services Terms of Service Provisions
- Website Developer Agreements
- Communications Decency Act Section 230 Immunity
- Personalization and Customer Experience in E-Commerce

Data Security & Privacy

- CCPA Regulations Compliance: Notice Requirements
- General Data Protection Regulation (GDPR)

Annotated Forms

- COPPA Privacy Policy
- Electronic Communication Systems Use Policy
- IT Resources and Communications Systems Policy
- Mobile Application Privacy Policy (General)
- Online Privacy Notice (Product or Services Sales Website)
- Social Media Privacy Policy (Short Form)
- Social Media Public Discourse Policy (With Guidelines)
- Website Terms of Use
- Website Terms and Conditions of Use (Website Provides Information and Services)
- Website Terms and Conditions of Use (Website Provides Information for a Fee)
- Website Terms of Use (Copyrighted Web Content)
- Acceptable Use Policy
- Subscriber Agreement and Terms of Use for Website with User-Generated Material
- Website Linking Permission Agreement (Long Form)
- Website Linking Permission Agreement (Short Form)

Checklists

- Electronic Communication Privacy Act Issues Checklist
- Privacy Policy Checklist
- E-Commerce Website Creation Checklist
- COPPA Flowchart
- Linking and Other Special Issues Checklist

Kavon Adli, Founder and Managing Attorney, The Internet Law Group

Kavon Adli founded The Internet Law Group (TILG) in 2008 to service the needs of the evolving e-commerce, online advertising and lead generation industries, quickly expanding the practice to cover a broad array of internet-related matters. Actively licensed in California since 1999, Kavon obtained his Texas law license in 2008 and currently represents clients located in a variety of U.S. states. He has served as TILG's managing attorney for the majority of his 21 year career, overseeing over 500 client engagements including LendingTree.com, West Publishing Group/Thomson Reuters, Debt.com, Ricola and the City of Huntington Park, to name a few. Kavon has advocated before and is admitted to practice in the California Supreme Court, the Ninth Circuit Court of Appeals, as well as the Northern, Central and Southern District Courts in California. Kavon has appeared on television and been published or quoted in numerous publications including ABC, Los Angeles Times, Law.com, Daily Journal, the Real Deal, LexisNexis and International Business Times.

Kavon earned a Bachelor of Arts in Philosophy (cum laude) from Dartmouth College in 1996 and is a 1999 graduate of the University of California at Berkeley School of Law (Boalt Hall). As a Los Angeles-based civil litigation attorney since 2000, Mr. Adli focused on commercial litigation matters, including contract, tort, partnership, advertising and other business disputes. In 2006 Kavon moved to Austin to become the in-house counsel and marketing department manager for a leading consumer finance advertiser and founder of the AchieveCard MasterCard. As General Counsel, Kavon handled legal matters for 30+ internet websites and the prepaid card program, including all areas of legal compliance, employment, contracts with advertisers, marketing partners, agencies and lead buyers, as well as the company call center.

During his free time Kavon is an avid sailor, skier, gardening and fitness enthusiast, and enjoys spending time with his wife and three dogs.

Jason Civalleri, Of Counsel, The Internet Law Group

Jason Civalleri is an attorney with deep experience with information technologies, including e-commerce, crypto-assets and blockchain, and data privacy/cyber-security. Jason advises internet-oriented clients on issues related to corporate formation, financing, employment, copyright and trademark, banking regulations, securities transactions, technology transactions, employment, and other general counsel services. He is designated a Certified Information Privacy Professional (CIPP-US) and a Certified Information Privacy Manager (CIPM) by the International Association of Privacy Professionals (IAPP).

In addition to his role as Of Counsel for The Internet Law Group, Jason serves as the Chief Compliance Officer of MyCrypto where he oversees privacy and money-handling compliance requirements for the premier client-side Ethereum crypto-currency wallet. Jason is a serial entrepreneur, having founded the SplytCore Foundation and Adason Financial, which are both still building innovative tools to serve the e-commerce and finance sectors (respectively). He is also proficient in programming in Python, JavaScript, and Solidity, and teaches a course on blockchain-related law at the Franklin Pierce School of Law at the University of New Hampshire.

Jason earned his Juris Doctor from the University of California at Irvine, where he was voted most entrepreneurial by his peers. He also obtained a Master of Business Administration at the Merage School of Business at UC Irvine, which awarded him Certificates of Excellence in entrepreneurship.

When he is not pursuing his professional passions of law, business and technology, Jason enjoys traveling, crafting beer, and reading philosophical literature.