PRIVACY POLICIES & A CHECKLIST FOR DRAFTING A PRIVACY STATEMENT

Excerpted from Chapter 26 (Data Privacy) of *E-Commerce and Internet Law: A Legal Treatise With Forms, Second Edition*, a 4-volume legal treatise by Ian C. Ballon (Thomson/West Publishing 2014)

ACC SoCal Presents
THE IN-HOUSE COUNSEL CONFERENCE
JANUARY 22, 2014
THE BEVERLY HILLS HOTEL
BEVERLY HILLS, CA

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles:
1840 Century Park East, Ste. 1900
Los Angeles, CA  90067
Direct Dial: (310) 586-6575
Direct Fax: (310) 586-0575

Silicon Valley:
1900 University Avenue, 5th Fl.
East Palo Alto, CA 914303
Direct Dial: (650) 289-7881
Direct Fax: (650) 462-7881

Ballon@gtlaw.com
<www.ianballon.net>
Google+, LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition* (Thomson West 2014 Annual Update), a 4-volume legal treatise by Ian C. Ballon, published by West LegalWorks Publishing, 395 Hudson Street, New York, NY 10014, (212) 337-8443, [www.ianballon.net](http://www.ianballon.net).
Ian Ballon represents Internet, technology, and entertainment companies in copyright, intellectual property and Internet litigation, including the defense of privacy and behavioral advertising class action suits. He is also the author of the leading treatise on Internet law, *E-Commerce and Internet Law: Treatise with Forms 2d edition*, the 4-volume set published by West (www.IanBallon.net). In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009) and serves as Executive Director of Stanford Law School's Center for E-Commerce.

Mr. Ballon, who practices in both Silicon Valley and LA, has brought or defended novel suits involving computer software, user generated content, rights in the cloud and in social media, links, frames, sponsored links, privacy and security, database protection, screen scraping and content aggregation, digital music, the Digital Millennium Copyright Act, rights of privacy and publicity, the enforceability of Internet Terms of Use and Privacy Policies and preemption under the CDA. A list of recent cases may be found at www.GTLaw.com/People/IanCBallon.

Mr. Ballon was named the Lawyer of the Year for Information Technology Law in the 2013 edition of Best Lawyers in America. In addition, he was the 2010 recipient of the State Bar of California IP Section's Vanguard Award and named new media lawyer of the year in 2012 by the Century City Bar Association. He is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also has been recognized by *The Daily Journal* as one of the Top 75 IP litigators and Top 100 lawyers in California and is regularly listed as a top Northern California and Southern California litigator. Mr. Ballon also holds the CIPP certificate for the International Association of Privacy Professionals (IAPP).
law and statutes. A checklist of issues that all businesses should consider is set forth below in section 26.14[3].

Before drafting or revising a privacy statement, readers are encouraged to read section 26.01, which provides an overview of data privacy law today and how it is evolving. Other sections of this chapter that may be relevant are identified in section 26.01 and in the footnotes to the checklist that follows.

Readers are also encouraged to review chapter 22 (Website Terms and Conditions) which analyzes both the substance and presentation of website contracts and policies, and chapter 27 on data security. In particular, readers may find it helpful to review the security compliance checklist set forth in section 27.11. A discussion of mobile-related issues is set forth in section 21.08. Mobile issues also are addressed in the California Attorney General’s guide, Privacy on the Go, which is reprinted in the appendix to this chapter, and in connection with the FTC's COPPA Rule in section 26.13[2]. Special issues associated with the use of social networks by employees and social media credentials are analyzed in section 58.06[6]. That section analyzes state laws enacted to restrict employer access to the social media credentials and communications of employees and job applicants.11 Additional privacy considerations associated with social networks may be found in chapter 51. Chapter 51 also addresses Internet safety, including child safety and state laws applicable to Internet dating sites.


The most important thing about a privacy policy is that it must reflect a company’s actual practices. The easiest and quickest way for a business to get into trouble is when its actual practices diverge from its stated practices, as evidenced by some of the enforcement actions brought by the FTC that are discussed in section 26.13[5].

The substance of a company’s privacy policy is much less important than its accuracy. Except for privacy policies governing businesses in the banking or health care industries or with respect to information collected from children or transferred from Europe, there typically are no specific policy provisions that must be adopted by site owners and service

11See infra § 58.06[6][C].
Despite this flexibility, many companies run into trouble—often unintentionally. A privacy policy is a living document that must be reviewed periodically. If a company adopts a policy that accurately reflects its practices today, six months or a year from now business or marketing practices or new technologies may render an otherwise accurate policy statement inaccurate.

A privacy policy should be written in clear, concise, language that average consumers will understand. An FTC staff report from early 2009 observed that privacy policies “have become long and difficult to understand, and may not be an effective way to communicate information to consumers.” This criticism is noteworthy and suggests that companies should rely upon shorter, more comprehensible policies to avoid eventual regulatory problems. Plain, clear language will also help a company in the event of litigation.

Ambiguity in an agreement, could undermine the value of a privacy statement to a company.\(^2\)

\[\text{Section 26.14[2]}\]


\(^2\)See In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1076–77 (N.D. Cal. 2012) (denying plaintiffs’ motion to dismiss claims in a putative class action suit where the court found some ambiguity in the defendant’s Terms and Conditions). In In re iPhone Application Litig., the court found commonly used privacy statement provisions to provisions to be unclear and therefore not support plaintiffs’ motion to dismiss, explaining:

On the one hand, the Agreement informs users that Apple may collect “non-personal information” including “zip code, area code, unique device identifier, [and] location” and the Agreement authorizes Apple to “collect, use, transfer, and disclose non-personal information for any purpose.” However, Apple also limits how it may utilize users’ “personal information” which it defines as “data that can be used to uniquely identify or contact a single person.” It does appear that there is some ambiguity as to whether the information collected by Apple, including the user’s unique device identifier, is personal information under the terms of the Agreement, and thus whether Apple’s collection and use of the information is consistent with the Agreement’s terms.

Additionally, . . . it is not clear that Apple disclaimed all responsibility for privacy violations because, while Apple claimed not to have any liability or responsibility for any third party materials, websites or services, Apple also made affirmative representations that it takes precautions to protect consumer privacy.

In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1077 (N.D. Cal. 2012).
There potentially is a fine line between detailed disclosure and complexity. Brevity may be criticized if material details are omitted, while granularity can be objected to because a policy with greater transparency is then too complex for the average consumer to understand. Both omissions and complexity may be cited by courts and regulators in imposing liability.

A privacy policy concerns information about consumers. Corporations do not have privacy rights.

As discussed in section 26.01, the FTC has noted in connection with behavioral advertising that the distinctions between PII and non-PII have ceased to be meaningful because of the number of ways that non-personally identifying information may be linked with other data and effectively identify an individual. It would be a mistake to overlook this perspective in drafting or revising a privacy policy, regardless of whether a company engages in behavioral advertising, because it reflects the broader thinking of policy makers at the FTC and likely emerging trends.

A privacy policy should disclose a company’s practices with respect to the collection, storage, use, and dissemination of personally identifying information and information that reasonably could be associated with a particular consumer or device, whether or not PII. In its final 2012 report, the FTC clarified that data is not deemed reasonably linked if a company takes reasonable measures to de-identify the data, commits not to re-identify it, and prohibits downstream recipients from re-identifying it.

What historically has been thought of as personal information may be anonymized (or de-personalized), while even anonymous data may become de-anonymized (or re-personalized) if enough data points are collected.

IP addresses, for example, identify a particular computer, rather than an individual user, but if a user has a static IP address linked to a unique domain name—such as the person’s name—it would not take much effort for a user to

---

*See infra § 28.06.
*See generally supra § 26.13[4].
deduce the identity of the person associated with the IP address. IP addresses generally are not considered PII in the United States, although courts may take precautions in protecting IP addresses in litigation.\textsuperscript{6}

Geolocation data similarly may disclose nothing more than the location of a mobile device or computer from which a site was accessed or may uncover that a person was somewhere other than where they claimed to be or reveal a person’s hobbies, interests, affiliations and associations.\textsuperscript{7} Geolocation data can be presented in an array of formats (such as coordinate or map data) and in some instances may be more precise than street name and name of a person’s home city or town.

Some of the data collected on a website may not be clearly personally identifying information but potentially could reveal the identity of a user or could be combined with other data to become personally identifying information (PII). For example, the particular pages visited by a particular unidentifiable user generally is not be PII, but if this information becomes linked to PII in a person’s profile once they log on to their account, then the particular sites visited by the person might cease to be anonymous data.

Site history and viewing patterns are not considered to be PII under most privacy statutes. However, statutes alone do

\textsuperscript{6}See, e.g., Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007) (ordering the collection of data from user logs on BitTorrent nodes, but requiring that the data be preserved in a manner that masked the IP addresses); see generally supra §§ 4.03[2], 4.12[18] (discussing the case), 26.03 (analyzing privacy rights in IP addresses).

\textsuperscript{7}Geolocation data has not been afforded substantial protection to date under U.S. privacy laws, although the FTC presently is studying the issue. See, e.g., In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1062–63 (N.D. Cal. 2012) (holding that the alleged disclosure to third parties of the unique device identifier numbers of Apple mobile devices, personal data stored by users on those devices and geolocation information did not involve an egregious breach of social norms and therefore was not actionable under California’s constitutional right to privacy and that geolocation data was not protected from disclosure under the Electronic Communications Privacy Act in a civil lawsuit); see also Boring v. Google, Inc., 362 F. App’x 273, 278–80 (3d Cir.) (affirming dismissal of plaintiffs’ Pennsylvania common law privacy claim based on the inclusion of photos of their house, garage and pool, which they alleged was located on a private road, in Google Maps, because the disclosure (which did not include the inside of their house) would not be highly offensive to a person of ordinary sensibilities), cert. denied, 131 S. Ct. 120 (2010); infra §§ 50.06[4] (geolocation data and the Electronic Communications Privacy Act), 58.06[7] (Fourth Amendment issues relating to geolocation data).
not dictate practices in this area. The FTC will look to consumer expectations based on what was disclosed to them in a privacy policy and elsewhere. Similarly, state law claims (or suits under California’s unique Constitutional right to privacy) generally will turn on reasonable consumer expectations. Using absolute statements in a privacy policy such as “Except as stated above, we will never share your information with others” or ambiguities—such as whether particular data about a person is or is not covered by the policy—should not be viewed as best practices.

All interactive websites collect information when they are accessed by users. Some of this information may be personally identifying information—such as a user’s name, address, birth date or other details that identify and distinguish one user from all others. Some may be non-personally identifying—such as aggregate statistics about a website that do not reveal information about any particular user. The fact that a website may be accessed by 1,800 people on a particular day, each of whom spent an average of five minutes on the site may be valuable data to a site owner or service provider and to its advertisers, but it does not implicate the privacy interests of consumers.

Where there is any ambiguity about whether particular data could be used to identify a particular person, it is best to disclose the site’s collection and storage practices, and the anticipated use and dissemination of the information. Some privacy policies, for example, describe collection practices for both PII and non-PII and explain, as appropriate, how non-PII may be used or combined with PII or to identify a given user, in contrast to aggregated or anonymous data.

Some sites also allow users to opt-out of certain information practices or block disclosure, including by establishing privacy settings that a user may configure based on his or her preferences.

A company should disclose both collection practices that are apparent (such as information provided in response to forms that call upon users to provide personally identifying information) as well as those that may not be evident to consumers (such as information that is automatically collected through the operation of a website). For example, a site should disclose how it uses cookies, web beacons and

---

*See supra § 26.07.*
other features that may collect personal and non-personally identifying information, what information is collected and how it is used.\(^9\) Sites that collect data from European Union residents also must comply with EU law requiring consent\(^9\).

In evaluating what information may be collected by a company, there are often gray areas. When confronting shades of gray, sunlight and transparency is the best policy. Because no particular policy is required, merely disclosing collection, storage, use and dissemination practices and then adhering to the terms of the stated policy is the best approach to avoid liability.

Transparency and full disclosure do not mean that a policy should be unduly long. Privacy policies need to be understood by consumers and therefore should be clear, well written statements in plain English with headings that accurately reflect the topics discussed. Privacy policies also should be easily printable so that users may review them in detail, at their leisure. A policy that is too long for most consumers to read or understand may create more problems than it solves.

Site, service and mobile providers ultimately should consider the level of sensitivity of data and their proposed uses for it in evaluating what level of disclosure may be required.

Companies also should consider implementing privacy by design and auditing their collection practices for uncurated data that may lead to unnecessary liability risks.\(^1\)

No two companies will have the same policies, practices and procedures with respect to the collection, use and dissemination of information. Different businesses have different uses for PII (as well as practices with respect to non-PII that nonetheless could identify a person and therefore should be disclosed). They also may have different corporate cultures and clientele.

Some companies may want to do everything possible with personal information. In the Internet advertising and promotions industry, for example, information typically is more valuable than in other industries where users would revolt if they thought that their personal information would even be

---

\(^9\)See infra § 26.03.
\(^{10}\)See supra § 26.04[17].
\(^1\)See supra § 26.01.
shared with others. Other entities may fall somewhere in between, using personal data for internal marketing purposes (or sharing it with affiliated entities) but not necessarily transferring it to unrelated third parties. Some will be content to simply analyze data and transfer only aggregate information to third parties.

In preparing a privacy policy, businesses may need to consider how to treat information collected from residents of different jurisdictions (and whether to do so under a single, unitary policy that complies with the laws of the most restrictive jurisdictions (such as the European Union and Canada), or under separate policies that allow a company to do the most permitted by law with personal data in each country or state where it operates). If a company uses separate policies for different jurisdictions, it must be careful to segregate data so that information collected under a more restrictive policy is not used pursuant to a more liberal one.

Although it is an important rule of thumb that whatever a company says it does with respect to the collection, storage, use and dissemination of information must be consistent with its actual practices, in point of fact, a company is free to do less with data than what is stated in a policy and not run into trouble. If the policy says a company may share information with third parties and in fact it does not do so, the company will not risk litigation or regulatory enforcement actions. A privacy policy sets a ceiling, rather than a floor, on what may be done with PII and information that could become associated with a particular consumer. As long as a company does not do more than is disclosed it will usually avoid trouble.

For this reason, some lawyers draft very liberal policies to allow companies maximum flexibility. For example, a site owner or service provider might say that it may transfer all data collected to third parties, which is a short but very broad statement that allows a company a great deal of flexibility in using user data. For some companies and in some industries, however, disclosing that data will be transferred to third parties can create public relations problems, leading to blog postings and other commentary critical of the site or service. Some companies therefore take a middle ground approach, identifying certain specific uses that they deem non-objectionable, but stating that information otherwise will only be used if specific permission is sought. The more restrictive a policy, the more important it is to make sure that
those responsible for compliance adhere to its terms.

Drafters should consider both current practices and likely future changes to craft a policy flexible enough to not require frequent material revision. When a policy is revised, information collected under an earlier policy cannot be handled pursuant to the terms of the new policy if they conflict in material respects, without risking liability or an FTC enforcement action. A site owner or service provider that makes material changes to its policy should either segregate user information—treating different data according to the policy under which it was collected—or seek express consent to treat a person's information under the terms of the new policy.

Some companies in fact do both. Old data is separated from newly collected information, while at the same time acceptance of the new policy is sought from existing users as they return to the site. As with data collected under different policies internationally, companies need to be careful that data collected under more restrictive terms is not used pursuant to more liberal policies. The more policies and guidelines that need to be followed, the more opportunity there is for a company to make a mistake. For this reason, some companies opt to treat all data subject to uniform policies, even if it means that opportunities to commercially exploit some PII are lost.

Some businesses do not take seriously enough the task of drafting and properly implementing a privacy policy and instead borrow from policies posted online or created for affiliate companies (even though those policies may bear little resemblance to a company's actual practices or intended future uses). A privacy policy may be enforced against a company (and is treated by the FTC as a promise to consumers) or defensively to show that a particular practice was disclosed, but rarely can it be used offensively by a business. Just as a company would not photocopy a form contract from an unrelated transaction every time it needed

---

12See supra § 26.13[6] (California law); see also supra § 26.13[5][C] (discussing the FTC's position on material changes).

13A privacy policy may be enforced against a company. Unless made part of Terms of Use or another contract, a company may not enforce rights against users based on the terms of the Policy, although a policy may negate expectations of privacy, which may be helpful in the event of litigation.
to sign an agreement with a business partner, a business should not use a standard form or copy another site’s privacy policy without carefully evaluating its applicability.

The starting point for drafting a privacy policy is to consider those laws that mandate the existence and substance the policy. Federal law provides specific direction for companies in the health care or financial services industries and for companies that target or knowingly collect personally identifying information from children.\(^\text{14}\) The U.S. Commerce Department likewise provides specific guidance on what must be included in a privacy policy that is intended to comply with the safe harbor principles for data transfer from the European Union.

For most other sites, the first place to look is to the laws of those states that require a privacy policy in connection with the collection of information from state residents (assuming that a site intends to collect information on a nation-wide basis and therefore must comply with all state laws).\(^\text{15}\)

California requires operators of commercial websites and online services that collect *personally identifiable information* over the Internet about individual consumers residing in California who use or visit the site, to conspicuously post a privacy policy that (1) identifies the categories of PII that the operator collects and the categories of third parties who may be given this information, (2) describes the process by which consumers will be notified of changes to the policy, (3) identifies its effective date, and (4) if applicable, describes the process by which an individual may review and request changes to information collected about her.\(^\text{16}\) California law also imposes other requirements on site owners with respect to the privacy and security of online data.\(^\text{17}\) Texas further requires that anyone requiring disclosure of a social security number must make available a privacy policy, which must disclose how personal information is collected, used and


\(^{15}\)State laws generally apply to out of state residents unless they are expressly preempted by Congress or implicitly by the Commerce Clause. See infra § 35.04.

\(^{16}\)See supra § 26.13[6][B].

\(^{17}\)See supra §§ 26.13[6][C], 26.13[6][D].
protected, who has access to it and how it will be disposed.\(^{18}\)

FTC guidelines on fair information collection practices and the Consent Judgment in *In re GeoCities, Inc.*, provide a potential roadmap of what the FTC would like to see in a privacy policy.\(^{19}\) FTC enforcement actions generally provide insight into the type of practices that should be avoided.\(^{20}\)

If a site is not targeted at children, it is often desirable to restrict access to the site to users who are 13 years or older. To avoid COPPA compliance, a site must not simply avoid targeting young children but may not knowingly collect personal information from minors younger than 13. Accordingly, a site or service may want to have in place procedures for purging PII and terminating users when knowledge is acquired.\(^{21}\)

The Child Advertising Review Unit (CARU) of the Better Business Bureau\(^{22}\) provides useful guidelines for sites targeted to children (as well as for sites that want to avoid inadvertently collecting PII from children under 13). Among other things, a site seeking to avoid collecting information from minors should use cookie files to prevent a child who was blocked from registering for a site based on the age listed from pressing the “back” button on his or her browser and simply signing on with a phony, older age.

A business also should evaluate to what extent it may be appropriate to include protections for the privacy and safety of minors older 13 years and older who are not subject to COPPA, but may require enhanced protection in appropriate

---

\(^{18}\)See supra § 26.13[8].

\(^{19}\)The provisions of that Consent Judgment need not be adopted in toto in order to avoid an FTC enforcement action. The GeoCities, Inc. Consent Judgment was intended in part to correct past practices and therefore presumably is stronger than what the FTC would have required of a business with no history of violations. More than a decade later, the principles incorporated in the settlement remain surprisingly relevant in evaluating privacy guidelines.

\(^{20}\)See supra § 26.13[5].

\(^{21}\)See supra § 26.13[2].

\(^{22}\)See http://www.caru.org/program/index.aspx; see generally supra § 26.13[2].
circumstances in the view of the FTC.  

Privacy policies typically include information on security. Some drafters are too enthusiastic in their expressions of concern for security. As born out by FTC enforcement actions, statements like “Security is our top priority” may be deemed privacy promises that will lead to enforcement actions if breached. Statements about security should be understated and include disclaimers noting that many things (such as viruses and hacker attacks) the site owner or service provider genuinely cannot control.

Sites also should disclose the circumstances under which they will reveal personally identifying information to third parties, including pursuant to subpoenas or court orders. Most sites usually draft these provisions carefully to avoid being sued by users for privacy violations. In Doe I v. Individuals, for example, the court held that a defendant had only a minimal expectation of privacy in communications made from her AT&T account because AT&T’s privacy policy made clear that “where permitted or required by law, [AT&T will] provide personally identifying information to third parties . . . without your consent . . . [t]o comply with court order, subpoena, or other legal or regulatory requirements.”

In addition to covering third-party disclosures, sites should ensure that restrictions on their own use of information are not so strict that they cannot use information in their possession or provide it to their lawyers or consultants in the event of litigation.

Where a privacy policy, Terms of Use or other notice make clear that particular user submissions will be treated as private, a court may decline to compel their production (and the site could risk liability for voluntarily doing so). In Viacom Int’l, Inc. v. YouTube, Inc., for example, the court construed the terms of YouTube’s user agreement as not authorizing the disclosure in discovery of the contents of

---

23 See supra § 26.13[2]; see also infra § 51.09 (Attorney General settlements and best practices for ensuring the safety of minors on social networks).

24 See infra § 27.06.


26 To avoid liability it may be advisable to include a disclaimer governing inadvertent disclosures or those compelled by court order.

videos marked private\textsuperscript{28} based on the Electronic Communications Privacy Act's prohibition against knowingly divulging the contents of any stored electronic communications on behalf of subscribers, subject to various exceptions that he deemed inapplicable including consent.\textsuperscript{29} In so ruling, Judge Stanton rejected plaintiffs' argument that users authorized the disclosure by assenting to YouTube's user agreement, which included provisions licensing YouTube to distribute user submissions in connection with its website and business, disclaiming liability for the disclosure of user submissions, and notifying users that videos they divulge online in the public areas of the website may be viewed by the public.\textsuperscript{30}

If a site includes personally identifying information licensed or acquired from other sites or services, it should review in-bound license agreements to verify the terms under which the data was provided and how it may be re-used. In general, FTC guidelines require that PII only be used in accordance with the terms of the policy pursuant to which it was collected.

Site owners or service providers that comply with the Digital Millennium Copyright Act by maintaining a notice and take down mechanism for copyright owners to report infringing material—which limits the liability of participating site owners and service providers\textsuperscript{31}—should disclose their practices even though the DMCA itself does not expressly require this. Specifically, if the site permits counter notifications it should disclose that notifications will be provided to account holders whose content is the subject of a notice and,

\textsuperscript{28}YouTube allows users to change the default setting, which otherwise makes their submissions publicly viewable, to mark particular video submissions as "private" and share those videos only with specified other users.


\textsuperscript{30}253 F.R.D. at 264–65. Judge Stanton ruled that the provision granting YouTube a license to video submissions authorized YouTube to post videos on its site, but was modified by the privacy designation given to individual submissions which restricted to whom videos could be shown. Similarly, a privacy policy provision warning users that any videos submitted "may be viewed by the general public" referred to information voluntarily disclosed online ("on discussion boards, in messages and chat areas, within your playback or profile pages, etc. . . . [which] becomes publicly available" and not to videos marked private. 253 F.R.D. at 265 nn. 9–11.

\textsuperscript{31}See 17 U.S.C.A. § 512; supra § 4.12.
likewise, that any counter notification will be submitted to the copyright owner who submitted the initial DMCA complaint.\footnote{A typical clause could read as follows: DMCA Infringement Notifications, Notices of Violations of Site Terms of Use and Other Communications Directed to Us. By submitting a Copyright Infringement Notification or other communication (including communications about content stored on or transmitted through the Website) you consent to have that communication forwarded to the person or entity who stored or transmitted the content addressed by your communication, in order to facilitate a prompt resolution. For Notices of Violations of Website Terms of Use or other communications (but not DMCA Infringement Notifications), upon request we will edit out your name and contact information. However, DMCA Infringement Notifications (including any personally identifying information set forth in the Notifications) will be forwarded as submitted to us without any deletions.}

If a site has other notice and takedown procedures in place, similar disclosures should be provided (assuming that the site or service finds it useful in resolving disputes and deterring fraudulent complaints to forward complaints and responses to those involved in a dispute).

The objective of a privacy policy—in addition to complying with laws or regulations that require them to be posted—should be to fully disclose a company’s practices to negate privacy expectations that otherwise could lead to an FTC enforcement action\footnote{See supra § 26.13[5].} or equivalent state action or litigation.\footnote{See infra § 26.15.} If affirmative assent is obtained to the terms of a privacy policy, it will be harder to argue at a later date that a user was not on notice of the site’s practices.

Obtaining express assent (either directly or through incorporation by reference) also is advisable for companies that seek to bind users to arbitration provisions and thereby avoid privacy related class action litigation.\footnote{See supra § 22.05[2][M] (analyzing arbitration provisions and class action waivers); infra § 26.15 (privacy class action suits).}

Click-through agreements also could be used to meet the EU Data Protection Directive’s requirement that consent be freely given, specific and unambiguous.

A privacy policy, however, need not be set up like a contract. Indeed, since privacy policies typically are enforced against a site owner and any protections a site owner or service provider would like to obtain from users (such as war-
ranty disclaimers and limitations on liability) usually may be included in Terms of Use, many sites opt not to provide users with another reason to sue them\textsuperscript{36} and simply treat

\textsuperscript{36}Some courts have held that a breach of contract claim may not be based on a posted privacy policy. See, e.g., Jurin v. Google Inc., 768 F. Supp. 2d 1064, 1073 (E.D. Cal. 2011) (dismissing with prejudice claims for breach of contract and breach of the duty of good faith and fair dealing arising out of the alleged breach by Google of its AdWords policy terms and conditions because a “broadly worded promise to abide by its own policy does not hold Defendant to a contract.”); Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196 (D.N.D. 2004) (holding that plaintiffs could not maintain suit against Northwest Airlines for breach of its privacy statement because it was not a contract, plaintiffs did not allege that they in fact had accessed, read, or relied upon it and plaintiffs did not allege any contractual damages arising from its alleged breach); In re Northwest Airlines Privacy Litig., 2004 WL 1278459 (D. Minn. 2004) (ruling the same way where plaintiffs alleged that they had relied on the privacy policy but had not actually read it).

Other courts have held that plaintiffs potentially could maintain breach of contract claims for alleged privacy policy violations, at least for purposes of stating a claim at the outset of a case. See, e.g., In re Easysaver Rewards Litig., 737 F. Supp. 2d 1159 (S.D. Cal. 2010) (denying a motion to dismiss claims for breach of contract and breach of the duty of good faith and fair dealing where plaintiffs alleged that they purchased flowers from a website subject to the Terms of Use, Privacy Policy and Rewards Policies posted on the site and that their personal financial information thereafter was transmitted to a third party in breach of these documents or, if permitted, that the relevant provisions were unconscionable); Smith v. Trusted Universal Standards In Electronic Transactions, Inc., Civil No. 09-4567 (RBK/KMW), 2010 WL 1799456 (D.N.J. May 4, 2010) (holding that the plaintiff in principle could assert a breach of contract claim based on alleged violations by defendants of their privacy policies, but granting defendants’ motion to dismiss because the plaintiff did not allege any loss flowing from the alleged breach); Meyer v. Christie, No. 07-2230-JWL, 2007 WL 3120695 (D. Kan. Oct. 24, 2007) (holding that while unilateral corporate policies generally do not support breach of contract claims, the plaintiff could sue for breach of a bank’s privacy policy where the plaintiff had a long-term relationship with the bank, in the course of which he relied on the bank to preserve his confidential information in accordance with its privacy policy, and where, when the bank solicited his financial information in connection with its request that he act as guarantor of loans to ERP, the policy “was part and parcel of its offer to make the loan to ERP”); In re Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 325–27 (E.D.N.Y. 2005) (holding that a privacy policy potentially can form the basis of a contract claim based on reliance, but granting defendant’s motion to dismiss where plaintiffs could not allege any loss from the breach). A contract claim, where available, may be easier for plaintiff than other potential claims that could be asserted. A plaintiff may recover in a breach of contract suit by showing a promise, breach and injury, rather than a reasonable expectation of privacy or other elements of state or
Privacy Statements as notices to consumers making clear in the document that it is not a contract. Others incorporate privacy policies by reference in Terms of Service and affirmatively seek click-through assent to both documents. For many online businesses, formal click-through agreements may be unnecessary and impractical. In addition, the FTC’s Consent Judgment in the GeoCities case underscores that merely posting a privacy policy accessible via federal privacy law claims. See supra §§ 26.05 to 26.13 (outlining potential claims under U.S. law); see also supra § 14.03[2] (addressing a contracting party’s duty of good faith).

Whether a privacy policy in fact can support a breach of contract claim likely will turn on the particular policy at issue, as well as the jurisdiction in which the claim is asserted. In more liberal jurisdictions, the failure to adhere to the terms of even a non-contractual privacy statement theoretically could give rise to claims in Litig., such as under California’s notoriously broad unfair competition statute (Cal. Bus. & Prof. Code §§ 17200 et seq.; supra § 25.04[3]) and Consumer Legal Remedies Act (Cal. Civ. Code §§ 1750 et seq.; supra § 25.04) or unique Constitutional right to privacy (supra § 26.07[2]), or in an FTC enforcement action. See supra § 26.13[5]. In at least one case, a court also allowed a claim to go forward where plaintiffs alleged conversion based on the alleged misappropriation of their private financial information, which was then used to make allegedly unauthorized debits from their financial accounts. In re Easysaver Rewards Litig., 737 F. Supp. 2d 1159 (S.D. Cal. 2010).

As a practical matter, however, plaintiffs to date have had difficulty framing viable claims in most instances, in large part due to the absence of damage or injury. See infra § 26.15.

While a site owner or service provider potentially may be held directly liable for own failure to adhere to the terms of its privacy policy under one theory of recovery or another, secondary liability likely would be preempted by the Communications Decency Act, 47 U.S.C.A. § 230(c); infra § 37.05. If a plaintiff were able to assert a contractual undertaking, however, it is possible that such an obligation could be viewed as outside the scope of CDA immunity. See Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009); see generally infra § 37.05. Many data privacy claims are dismissed on the merits. See infra § 26.15. Nevertheless, the cost of litigation and adverse publicity surrounding privacy suits argue in favor of taking proactive measures. For all of these reasons, site owners and service providers may find it beneficial to include a binding arbitration provision in consumer contracts that broadly extends to its privacy practices, to limit the risk of class action litigation. See supra § 22.05[2][M][vi] (drafting tips).

See supra § 22.03.

Business decision-makers often are resistant to law department suggestions to use click-through agreements because of the perception that website traffic may be adversely affected by inhibiting or delaying the speed of user access to information. For an analysis of the legal consequences of failing to use click-through agreements, see supra § 21.03.
links set up on the homepage at each location where personal information is collected generally will satisfy the FTC.

To the extent contractual, general statements that consumers would understand not to be representations, could be construed as mere puffery.\textsuperscript{39} “The distinguishing characteristics of puffery are vague, highly subjective claims as opposed to specific, detailed factual assertions.”\textsuperscript{40} While the FTC recognizes puffery in the context of advertising claims,\textsuperscript{41} as a practical matter both the FTC and courts are likely to analyze statements in a privacy policy more closely because consumer expectations will differ in evaluating a privacy statement (which is intended to be a disclosure of a company’s practices, not a marketing document) than in considering statements made in connection with advertising. While privacy policies serve a public relations function, they are fundamentally consumer disclosure documents, not advertising. Consumer expectations also may be harder to discern given the changing nature of technology and business models.

\textsuperscript{39}See, e.g., \textit{In re Heartland Payment Systems, Inc. Customer Data Security Breach Litig.}, 834 F. Supp. 2d 566, 590–94 (S.D. Tex. 2011) (holding certain representations about a company’s security practices in S.E.C. filings, on its website and elsewhere amounted to puffery, while finding other statements to be potentially actionable misrepresentations), rev’d in part on other grounds sub nom \textit{Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.}, 729 F.3d 421 (5th Cir. 2013); infra § 27.07 (analyzing the case and the specific statements at issue in greater detail in the context of data security breach litigation). Among other things, the court found the following to be promises that Heartland would not intentionally share personal information with others that, while not puffery, were not relevant to the data breach at issue in the case:

- “we have limited our use of consumer information solely to providing services to other businesses and financial institutions,” and
- “[w]e limit sharing of non-public personal information to that necessary to complete the transactions on behalf of the consumer and the merchant and to that permitted by federal and state laws.”

\textit{Id.} at 593.

\textsuperscript{40}\textit{Haskell v. Time, Inc.}, 857 F. Supp. 1392, 1399 (E.D. Cal. 1994).

\textsuperscript{41}“Puffing refers generally to an expression of opinion not made as a representation of fact. A seller has some latitude in puffing his goods, but he is not authorized to misrepresent them or to assign to them benefits they do not possess . . . . Statements made for the purpose of deceiving prospective purchasers cannot properly be characterized as mere puffing.”

\textit{In re Wilmington Chemical Corp.}, 69 FTC 828, 865 (1966); see generally infra § 28.03[2] (FTC advertising guidelines); supra § 6.12[5][B] (analyzing puffing in the context of Lanham Act false advertising claims).
Where a privacy policy is made part of a binding contract, such as Terms of Use, the policy may be interpreted more strictly. Contracts tend to be construed against drafters and narrowly to the extent they restrict the rights of consumers. Privacy policies otherwise would merely set reasonable expectations under most of the privacy laws likely to be applied to evaluate non-contractual privacy policy. While privacy laws impose different specific requirements and in all cases provisions should be carefully and clearly drafted, a site may have more leeway if its compliance with its Privacy Policy is evaluated by reference to whether consumers had a reasonable expectation of privacy based on the terms of the disclosure, rather than whether the site adhered to contractual obligations to users. Non-contractual privacy terms also may be helpful to a site or service in a wide array of litigation where clarity of disclosure may help establish knowledge, notice or consent.\(^{42}\)

Some lawyers are uncomfortable de-linking a privacy policy from a Terms of Use agreement that includes liability limitations and warranty disclaimers or binding arbitration provisions\(^{43}\) that could prove helpful if a site is sued for a privacy violation. This concern may be addressed, however, by broadening the scope of those provisions in the TOU agreement to cover any suit arising out of the formation, performance, or breach of the contract or use of the site or service.

An arbitration provision that encompasses all claims aris-

\(^{42}\)For example, in *Mollett v. Netflix, Inc.*, No. 5:11-CV-01629-EJD, 2012 WL 3731542 (N.D. Cal. Aug. 17, 2012), the court dismissed plaintiff’s complaint under the Video Privacy Protection Act and analogous California law where Netflix’s privacy statement provided that:

You are responsible for maintaining the confidentiality of your account information and for restricting access to your computer or device through which you access your Netflix account. If you disclose your password to anyone or share your account and/or devices with other people, you take full responsibility for their actions.

*Id.* at *3. The court found that any information displayed to third parties who the subscriber allowed to access the subscriber’s Netflix account or a device connected to it (1) amounted to disclosures to the consumer herself (Mollet) and (2) even if it amounted to a disclosure by Netflix to a third party, it was not made knowingly or willfully by Netflix. The court explained that “posting a privacy policy cannot relieve Netflix of its duty to comply with the VPPA. It does confirm, however, that the Plaintiffs knew that by allowing access to their device they were making the choice to also allow others access to their PII.” *Id.*

\(^{43}\)See supra § 22.05[2][M].
ing under or relating to the formation, performance or breach of the agreement, including use of a site (potentially combined with a waiver of class remedies) likewise should be broad enough, if included in TOU, to compel arbitration of privacy disputes with users, and thereby avoid class action litigation.\(^4\)

On the other hand, obtaining express consent to an arbitration clause (or expressly incorporating a Privacy Statement in a contract where affirmative assent is obtained) could strengthen the argument that data privacy claims should be subject to arbitration, just as affirmative consent may make it more difficult for a user to allege that he or she was unaware of a site’s practices.

Whether a site seeks affirmative assent or merely posts its Privacy Statement ultimately depend on a number of considerations.

In addition to posting an initial Privacy Statement, companies need to establish practices and procedures for amending the Statement over time. The process for modifying a privacy statement, like updating Terms of Use,\(^4\) can be controversial because lawyers may want to provide more robust forms of notice to users than marketing or business people. While a privacy policy need not be more than merely a policy statement, and therefore (unlike a contract) assent need not necessarily be obtained, it is important that users be given notice of new terms for those terms to be deemed binding and to effectively negate expectations of privacy.\(^4\) Ideally, a site or service should email users when a privacy policy changes, prompt them to view the new policy upon logging in to an account the first time after it is posted, or, through use of cookies, alert them of the new policy the first time they log on to the site after the new policy has been posted. Some site owners will post a prominent notice on the homepage alerting users that a new policy will take effect in thirty days (or at some specified time in the future) and urging them to review the new policy. Express assent, of course, is always preferable, and makes it more difficult for users to assert that they were unaware of a policy in the event of litigation.

\(^4\)See supra § 22.05[2]{M} (arbitration provisions and class action waivers); infra § 26.15 (privacy class action suits).

\(^4\)See supra § 22.04.

\(^4\)See supra §§ 26.05, 26.09, 26.11, 26.12.
California law provides that the means used to notify users of material updates must be disclosed in the actual privacy policy.\(^47\) Inferentially, notice need not be provided for non-material changes. An immaterial change presumably means one that a site owner does not intend to enforce against a consumer (since a modified policy would not likely be enforced against a consumer who had no notice of the new terms).

A privacy policy may be deemed to create heightened privacy expectations that could defeat efforts to compel the identity of an anonymous or pseudonymous users through judicial process\(^48\) or justify disclosure.\(^49\) Some courts have

\(^{47}\)See supra § 26.13[6]; see also supra § 26.13[5][C] (discussing the FTC’s position on material changes).

\(^{48}\)See, e.g., Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726 (9th Cir. 2011) (upholding a motion to quash production of the stored communications of a foreign resident where Hotmail’s subscriber agreement provided that disclosures of user emails would be made in accordance with U.S. law and under ECPA no exception allowing disclosure applied); Cornelius v. Deluca, No. 1:10-CV-027-BLW., 2011 WL 977054 (D. Idaho Mar. 15, 2011) (declining to order disclosure of the identity of a poster where the defendant’s First Amendment rights were found to outweigh the plaintiff’s need for discovery because, among other things, the defendant’s website Privacy Policy and Terms of Use created heightened privacy expectations on the part of its users); McVicker v. King, 266 F.R.D. 92 (W.D. Pa. 2010) (declining to compel the disclosure of the identity of bloggers based, in part, on the fact that the Terms of Use and Privacy Policy of the site where the blog posts were made created an expectation of privacy that user information would be used “only in very limited situations.”); see generally infra § 37.02 (analyzing case law compelling and declining to order the disclosure of the identity of anonymous or pseudonymous Internet speakers). Significantly, in McVicker v. King, 266 F.R.D. 92 (W.D. Pa. 2010), the relevant Privacy Policy disclosed that third parties such as email service providers could access user information and “[t]he Company may also disclose your information in response to a court order, [or] at other times when the Company believes it is reasonably required to do so . . . .” Id. at 96. The court, however, found disclosure permissible “only in very limited situations” based on this and other language in the Policy, including the statement that “[p]rotecting consumer privacy online is important to us. By taking steps to protect the privacy of our members, we also hope to increase members’ confidence in the site and as a result, increase their online activity.” Id. By contrast, in Doe I v. Individuals, 561 F. Supp. 2d 249 (D. Conn. 2008), the court compelled the disclosure of the identity of a Doe defendant based in part on a similar notice as the one cited in McVicker which warned users that their identity could be disclosed in response to a court order. In that case, the Privacy Policy made clear that the service provider “where permitted or required by law, [will] provide personal identifying information to third
also specifically considered whether disclosures in a privacy policy could amount to a waiver of a person’s First Amendment right to anonymity.\textsuperscript{50} Whether a provision amounts to

\begin{quote}
parties . . . without your consent . . . [t]o comply with court order, subpoenas, or other legal or regulatory requirements.” On balance, it is unclear from the brief description in the opinion whether the court in \textit{McVicker} simply assumed that the existence of a Privacy Policy created heightened privacy expectations (which would not be a reasonable conclusion, since most commercial sites have policies that disclose their practices) or whether the court’s holding was based on a finding that the broad assurances set forth in the document trumped the specific provision disclosing that a user’s identity would be revealed in response to a court order.
\end{quote}

\textsuperscript{49}See, e.g., \textit{Faconnable USA Corp. v. John Does 1-10, Civil Action No. 11-cv-00941-CMA-BNB}, 2011 WL 2015515 (D. Colo. May 24, 2011) (declining to modify an order allowing expedited third party discovery into the identity of anonymous posters who modified Wikipedia articles on M1 Group and Faconnable alleging that the company financially supported Hezbollah, which has been labeled a terrorist organization, or order that separate notice be provided to them, where, among other things, the anonymous defendants’ Service Agreement with Skybeam, the service provider to which the subpoena was directed, “allow[ed] Skybeam to disclose the identity of its subscribers pursuant to ‘legal process’ and d[id] not require Skybeam to give its subscribers advance notice when it intends to make such a disclosure.”), \textit{vacated}, 799 F. Supp. 2d 1202 (D. Colo. 2011) (vacating the earlier order because the plaintiff’s voluntary dismissal of the action deprived the service provider of the right to challenge the magistrate judge’s ruling on the merits); \textit{Doe I v. Individuals}, 561 F. Supp. 2d 249 (D. Conn. 2008) (compelling disclosure where the Privacy Policy made clear that the service provider “where permitted or required by law, [will] provide personal identifying information to third parties . . . without your consent . . . [t]o comply with court order, subpoenas, or other legal or regulatory requirements.”); see generally infra § 37.02 (analyzing anonymity and John Doe suits).”

As explained by the court in \textit{Faconnable}, “[t]here is no reason for a court, presented with a complaint asserting a plausible claim for relief, to take greater care than has been taken by the anonymous poster to protect his anonymity or to assure prior notice of a subpoena.” \textit{Faconnable USA Corp. v. Does 1-10, Civil Action No. 1-cv-00941-CMA-BNB}, 2011 WL 2015515, at *8 (D. Colo. May 24, 2011).

\textsuperscript{50}See, e.g., \textit{Sedersten v. Taylor}, No. 09-3031-CV-S-GAF, 2009 WL 4802567 (W.D. Mo. Dec. 9, 2009) (declining to find that a third party’s right to anonymity was waived by provisions in the Privacy Policy on the website for The Springfield News-Leader where the comments at issue had been posted). In general, a person may waive his or her First Amendment right to free speech. See, e.g., \textit{Snepp v. U.S.}, 444 U.S. 507 (1980); see also \textit{Leonard v. Clark}, 12 F.3d 885, 889–90 (9th Cir. 1993) (noting that a waiver of First Amendment rights must be knowing, voluntary and intelligent). However, “courts indulge every reasonable presumption against waiver.” \textit{Aetna Ins. Co. v. Kennedy to Use of Bogash}, 301 U.S. 389,
a waiver or creates heightened privacy expectations should turn on the language of the provision and whether adequate notice was provided or assent obtained from the user.\footnote{Notice and assent are analyzed throughout this chapter and in terms of contract law in sections 21.03 and 21.04.}

While a higher standard may be applied for a waiver of constitutional rights, notice—in the form of disclosure in a privacy policy and an email sent to subscribers, with the right to opt out of data sharing—was deemed sufficient in one case for a court to infer consent, and dismiss plaintiff’s claims under the Electronic Communications Privacy Act, and hold that plaintiff did not have an objectively reasonable expectation of privacy to support his claim for the tort of intrusion on seclusion, where the court found adequate notice had been given that the ISP collected user browser data through cookies and web beacons and provided this information to a third party advertiser.\footnote{See Deering v. CenturyTel, Inc., No. CV-10-63-BLG-RFC, 2011 WL 1842859 (D. Mont. May 16, 2011); see also Kirch v. Embarq Management Co., No. 10-2047-JAR, 2011 WL 3651359, at *7–9 (D. Kan. Aug. 19, 2011) (holding, in granting summary judgment for the defendant, that the plaintiffs consented to the use by third parties of their de-identified web-browsing behavior when they accessed the Internet under the terms of Embarq’s Privacy Policy, which was incorporated by reference into its Activation Agreement, and which provided that de-identified information could be shared with third parties and that the Agreement could be modi-}

51

While a higher standard may be applied for a waiver of constitutional rights, notice—in the form of disclosure in a privacy policy and an email sent to subscribers, with the right to opt out of data sharing—was deemed sufficient in one case for a court to infer consent, and dismiss plaintiff’s claims under the Electronic Communications Privacy Act, and hold that plaintiff did not have an objectively reasonable expectation of privacy to support his claim for the tort of intrusion on seclusion, where the court found adequate notice had been given that the ISP collected user browser data through cookies and web beacons and provided this information to a third party advertiser. Certain claims based on the absence of authorization also may be negated where a
privacy statement discloses that particular practices will be employed by a site or service.\(^53\)

In *Suzlon Energy Ltd. v. Microsoft Corp.*,\(^54\) the Ninth Circuit rejected the argument that a foreign defendant had impliedly consented to the disclosure of emails stored by Microsoft in his Hotmail account on servers in the United States where Hotmail’s service agreement stated that user emails would only be disclosed according to U.S. law (and


\(^54\) *Suzlon Energy Ltd. v. Microsoft Corp.*, 671 F.3d 726 (9th Cir. 2011).
other circumstances not relevant to the case), and U.S. law prohibited an entity that provides electronic communication services to the public from disclosing the contents of its stored communications. The panel cited approvingly in dicta the proposition that implied consent, where applicable, rests on a theory of waiver,55 which could not be found based on the terms of Hotmail’s subscriber agreement.

On the other hand, in In re § 2703(d) Order,56 the court held that Twitter subscribers, who objected to the release of non-content data to the government pursuant to a sealed turnover order in connection with the government’s WikiLeaks investigation, had consented to the disclosure when they clicked on the “Create My Account” button and thereby consented to Twitter’s terms of use in a binding clickwrap agreement.57

In addition to posting Privacy Statements, some businesses opt to participate in self-regulatory compliance programs—or “seal” programs because participants may display a seal on their site attesting to their compliance—such as those run by TRUSTe, the Better Business Bureau Online or the Direct Marketing Association, which impose specific guidelines for businesses to follow and audit their compliance. Unless there is an important marketing benefit to a company to be able to display a seal showing compliance, few companies participate in these type of programs except to the extent required to do so by the safe harbor provisions of the Children’s Online Privacy Protection Act58 or the Safe Harbor Principles for transferring data from the European Union to the United States.59

The process of drafting a privacy policy should involve extensive review of a site’s actual practice and procedures (both current and anticipated), interviews with those persons responsible for collecting, using or disseminating third party information, and education and training to ensure that the

---


56In re § 2703(d), 787 F. Supp. 2d 430 (E.D. Va. 2011).

57In re § 2703(d), 787 F. Supp. 2d 430 (E.D. Va. 2011).

58See supra § 26.13[2].

59See supra § 26.04[14].
policy is properly implemented. To properly implement a privacy policy, legal, business, marketing and technology executives all must work together.

To the extent possible, a business should adopt the principles reflected in current draft FTC and Commerce Department recommendations.60

Cases analyzing privacy rights are set forth in section 26.15.

A checklist of issues to consider in drafting or updating a privacy statement based on current law and regulatory trends is set forth in the following subsection.

Those drafting privacy policies for financial institutions should also refer to the Model Consumer Privacy Notice Online Form Builder found at http://www.federalreserve.gov/bankinginfo/privacy_notice_instructions.pdf.


Is a Policy Required?

• Does a business collect personally identifying information (or information that reasonably could become associated with a particular consumer or device) online?
  □ If not, it may be able to avoid many statutory obligations that otherwise arise,1 although off-line representations should be reviewed to make sure the company has not made representations about its privacy practices that should be addressed.
  □ Is the site targeted to individuals or business?
    — Business information may be confidential but it does not necessarily raise privacy issues unless it includes personally identifying information of consumers.
    — A B2B site is unlikely to need a privacy policy unless it is collecting personal information from consumers.

• What information does the site collect (and what will it collect in the future)?

60See supra § 26.13.

[Section 26.14[3]]

How will the site use the information it collects (both today and in the future)?

To what third parties will the information be provided (both today and in the future)?

Is a site obligated by U.S. law to post (or otherwise provide) a privacy statement?²

—is it a “financial institution” within the meaning of the Gramm-Leach-Bliley Act?³

— Does it provide a financial product or service for use for “personal, family or household purposes”?²

— If it is subject to GLB, relevant regulations issued by the FTC, SEC and other regulatory agencies should be reviewed for compliance.

Does it operate in the health care industry?⁴

— Is it a health plan, health care clearinghouse or health care provider who transmits any health information in electronic form, and legally obligated to protect “individually identifiable health information”?⁴

Does it collect information from children under age 13?⁵

— Can it avoid compliance with the Children’s Online Privacy Protection Act by targeting only people 13 years or older, and not knowingly collecting personal information from children?

Is the site required to post a policy to participate in the Safe Harbor program for trans-

— Where a privacy statement is mandated under federal law in the health care or financial services industries or for information collected from children, the terms of the policy will be dictated in part by implementing regulations.

²See 15 U.S.C.A. § 6801; 16 C.F.R. §§ 313.1 to 313.13 and Appendix A; see generally supra § 26.11.

³See 42 U.S.C.A. §§ 1320d et seq.; 45 C.F.R. §§ 160 to 164; see generally supra § 26.12. The privacy requirements imposed in connection with individually identifiable health information were not yet in effect as this chapter went to press.


Pub. 1/2014
ferring data from the European Union to the United States?\(^6\)

- Does the site or service collect personally identifying information over the Internet from California residents?\(^7\)

- Is the site directed at consumers?
  - Does the site actually collect personal information from consumers?
    - If so, what does it do with the information?
    - Is personal information provided to any third parties?

- If not legally required, is a policy necessary or appropriate?
  - Is there a marketing benefit to posting a policy? Even where a policy is not required because PII is not collected, a company may find it useful to post a policy on a site targeted to consumers to reassure them that their information will not be collected, transferred to third parties or otherwise used.

**Drafting the Policy**

- Consider cost, flexibility and corporate culture
  - Policies that are either very strict or very lax are easiest to draft because less time needs to be spent evaluating a company’s practices.
  - Most companies’ actual practices with respect to PII are likely to change over time. However, material changes to privacy policies should not be made unless restricted to PII collected after the date the new policy takes effect or with express consent.\(^8\)
  - Policies in which a company retains the maximum flexibility to use PII and transfer it freely to third parties allow a business to change practices over time without having to make material changes to their privacy policies or segregate data based on differing levels of permission obtained under different policies.

\(^6\)See supra § 26.04[14].

\(^7\)See supra § 26.13[6].

\(^8\)See supra § 26.14[2].
Depending on the industry, policies that allow a company maximum flexibility to use and transfer PII may be viewed negatively by consumers and impact the success of a site or service.

Strict policies may be difficult and expensive to implement.

Absent use of a liberal policy, sites that offer a wide variety of services may need to explain in detail the different ways in which information is collected, stored, used or provided to third parties, which may require a lengthy statement.

More complex policies may be more difficult for employees to implement and therefore increase the risk of breach and hence regulatory enforcement actions or litigation.

- All policies expose a company to liability if not actually implemented as written.
- Will more than one policy potentially be applicable to a user? If so, consider how privacy statements will inter-relate so that it is clear to users (and any subsequent reviewing courts) will statement controls in a given situation.
- Assess industry standards
  - In the absence of controlling law, reasonableness for purposes of state law or FTC enforcement actions may be judged by common industry practices.⁹
  - Evaluate trade group guidelines, if any.
  - Review the recommended practices of privacy advocacy groups
    - The Child Advertising Review Unit (CARU) of the Better Business Bureau has guidelines and information available on its site for the collection of information from children, verifiable parental consent and CARU’s safe harbor program
    - TRUSTe is another valuable source of guidance on privacy issues
    - Helpful resources for drafting a privacy

⁹See supra § 2.05.
Technical Issues and Adequacy of Disclosure

- Have all those with responsibility for collecting, using, storing or disseminating user information (or their managers) been consulted to ensure that any statement accurately discloses a company’s practices?
- What are the ways in which in which information is collected actively on the site (and what categories of data are collected)?
- In what ways is information passively obtained from users?
- Should particular practices, such as the use of cookies, third party cookies, flash cookies (or LSOs) or web beacons be specifically identified in a privacy statement?
- Is compliance with the European Union Directive governing cookies required by the site?\(^\text{10}\)
- What is done with the information collected? Who is it shared with?
- Should the policy link to the NAI webpage for opting out of behavioral advertising?
- Does the website, online service or mobile app provider disclose its practices with respect to “Do Not Track” settings in its privacy policy, as required by California law?\(^\text{11}\)
- Plan for compliance effective January 1, 2015 with California’s “Online Eraser” law for information or content from minors.\(^\text{12}\)
- What is the site’s practice’s with respect to aggregate or so-called de-identified or anonymous data?
  - □ Has the site evaluated the potential risks that anonymized data may be re-personalized and what disclosures, if any, are required?
- Does the site collect geolocation data,\(^\text{13}\) IP addresses or other data points that individually may not

\(^\text{10}\) See supra § 26.04[17].
\(^\text{11}\) See supra § 26.13[6][B].
\(^\text{12}\) See supra § 26.13[6][F].
\(^\text{13}\) See supra § 26.14[2] (and other sections of the treatise referenced there).
identify a person but collectively could reveal personal information?

- Are users allowed to opt out of any information collection practices or otherwise configure privacy settings?
- Are there material differences with respect to the information collected or used when a site is accessed from a mobile device rather than a computer?
  - If so, how is that information communicated to users?
    - Mobile app providers, like operators of websites and online services, are required to comply with California’s Online Privacy Protection Act of 2003.

**Specific Categories of Information**

- Ensure that the requirements of all the applicable laws listed under the section “Is A Policy Required?” are complied with.
- Evaluate practices targeted at teenagers who are not subject to COPPA, but may require heightened privacy, safety and security protections in the view of the FTC.
- Review the privacy policies of other companies in the industry
  - Privacy statements should reflect the actual practices of a company and its corporate culture and therefore should not simply be copied from other sites.
- Does the policy provide that personal information may be transferred to third parties in the event of sale of the business, transfer of assets, or bankruptcy?
- Will the site allow consumers access to records maintained about them?
  - If so, the process must be disclosed under

---

14Cal. Bus. & Prof. Code §§ 22575 et seq.; see generally supra § 26.13[6]. Readers may also wish to review Privacy on the Go, which is reprinted in the Appendix to this chapter.

15See supra § 26.13[2][H]; see also infa § 51.09 (Attorney General settlements and best practices for the safety of minors on social networks).

16See supra § 26.13[5].
California law (by California businesses or to California residents)\(^\text{17}\)

- Access is promoted by the FTC but is not necessarily required for companies not operating in Europe that are not otherwise compelled to post privacy statements by specific federal statutes.

- Does the policy include an “effective date” and other provisions required by California state law;\(^\text{18}\)

- Does the policy list physical and email addresses (or toll free telephone and fax numbers) on the first page, accessed from a link that includes the words “Your Privacy Rights” or otherwise comply with California’s personal information transfer disclosure statute (if personal information is provided to third parties)?\(^\text{19}\)

- Will the site collect information from users in connection with credit card transactions?\(^\text{20}\)

- Has the site, service or mobile device or app provider adequately accounted for uncurated data?\(^\text{21}\)

- Is the policy consistent with what the site owner says about its collection and use practices elsewhere on the website (or in representations off-line)?

- Is the policy consistent with contractual obligations owed to third parties?

- Is the policy applicable to a location where users may be interacting directly with third parties such that a disclosure and potentially a link to another privacy statement should be provided?

- Will the site subject its practices to an outside auditor, seal program or other independent recourse (or third-party enforcement) mechanisms?

- Businesses that do not plan to transfer personal data to third parties may find it easier to simply sign up with a seal program such as those operated by TRUSTe or BBBOnline, which provide sample privacy

\(^{17}\)See supra § 26.13.

\(^{18}\)See supra § 26.13[6].

\(^{19}\)See supra § 26.13[6][D].

\(^{20}\)See supra § 26.13[6][E].

\(^{21}\)See supra § 26.01.
policies and allow use of a seal that may be displayed on a company’s homepage (and which may have a marketing benefit for participants).

- Enforcement mechanisms are required by the Safe Harbor Principles but generally not otherwise under U.S. law.
- Some businesses may find third-party regulatory mechanisms too restrictive.

**International Issues**

- Does a site (or its owner) operate in Europe?²²
  - Which national laws must it comply with?
  - How will the site address the EU Cookie Directive?²³
  - Will data from different jurisdictions be segregated?
  - Will data be transferred to the United States?
    - Does the policy comply with the Safe Harbor Principles?²⁴
    - Does the policy comply with the EU Model Contract Clauses?²⁵
    - Does the policy comply with the national law of an EU Member State?²⁶

**External Implementation and Presentation:** How will the policy be communicated to the public?

- U.S. law and industry practice validate posted statements accessible via a link from a site’s homepage.
- Many businesses also provide “Privacy” links at every location on a site where personal information is sought from consumers, which is the FTC’s preferred approach.
- Particular companies may find it beneficial (or may be required) to provide notice by U.S. mail or other offline means.

---
²²See supra § 26.04.
²³See supra § 26.04[17].
²⁴See supra § 26.04[14].
²⁵See supra § 26.04[15].
²⁶U.S. businesses operating in Europe generally must subject themselves to EU law, enter into the model contract or comply with the U.S. Safe Harbor Principles that are subject to FTC enforcement. See supra §§ 26.04[14], 26.04[15].
Some sites incorporate by reference or include privacy provisions in click-through contracts or Terms of Use.\(^{27}\)

- Businesses that use click-through contracts may specifically address the collection of information in a separate screen (or series of screens), or ask consumers to provide assent in a single “click” to both documents (following text such as “Click here to accept and agree to be bound by Company’s Terms of Use contract and Privacy Policy”).

- Where separate screens are used (or a second “click” is requested), some sites use default settings with the default set to acceptance rather than being blank and requiring the user to take affirmative steps. This approach may not comport with laws in the EU countries, and may no longer be viewed as a “best practice” in the United States.

- Passive methods for obtaining assent may be inadequate absent actual notice to negate reasonable expectations of privacy under state law.\(^{28}\)

- Many companies prefer not to incorporate privacy policies into user contracts because privacy policies are more likely to be enforced against a company than by it.\(^{29}\)

- If express assent is not obtained, should a site adopt “opt-in” or “opt-out” procedures for inferring consent?

- Businesses typically favor opt-out procedures which require a consumer to affirmatively notify the site if he or she does not consent to a particular use of personal information.

- Opt-in procedures are usually disfavored by

\(^{27}\) See supra § 22.03. Terms and Conditions are analyzed in chapter 22.

\(^{28}\) See supra §§ 26.07, 26.08.

\(^{29}\) See supra § 22.03[2].
business people because few people typically respond.\textsuperscript{30} EU member countries generally require opt-in consent.

**Security**
- What measures will be adopted to ensure the security and integrity of personal data?
- Does the company have a separate information security policy?\textsuperscript{31}
  - What internal procedures have been adopted to comply with state security breach notification laws, in the event of a security breach?\textsuperscript{32}
    - Will the company adopt its own information security policy to provide alternative notice in the event of a breach?
- Is the policy drafted to negate unreasonable security expectations, in the event of hacker attacks or other unpreventable circumstances?\textsuperscript{33}
- In conjunction with drafting or revising a privacy policy, readers should review the security checklist set forth in section 27.08[13].

**Modifications**
- How will the site’s collection, use and dissemination practices change over time? How material

\textsuperscript{30}Congress adopted an opt-in procedure in 1999 amendments to the Driver's Privacy Protection Act of 1994 (18 U.S.C.A. §§ 2721 to 2725), the constitutionality of which was upheld on other grounds under the Commerce Clause by the *U.S. Supreme Court in Reno v. Condon*, 528 U.S. 141 (2000); see generally supra § 26.05. While Congress undoubtedly could compel use of opt-in procedures pursuant to its power to regulate data in interstate commerce, there is at least some question about whether the FTC could do so in implementing more general federal privacy guidelines. *See U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224 (10th Cir. 1999) (invalidating under the First Amendment an opt-in procedure adopted by the FCC to protect unspecified privacy interests), *cert. denied*, 350 U.S. 1213 (2000). In contrast to the DPPA, Congress adopted an opt-out procedure for “financial institutions” in the Gramm-Leach-Bliley Act. *See* 15 U.S.C.A. § 6802; see generally supra § 26.12[2]. An opt-out mechanism also is provided for under the Safe Harbor Principles applicable to the transfer of data from the European Union to the United States. *See supra* § 26.04[14].

\textsuperscript{31}See infra §§ 27.08[13], 27.11.

\textsuperscript{32}See infra § 27.08.

\textsuperscript{33}See supra § 26.13[5], infra § 27.07.
changes will be made must be set forth in the policy.\textsuperscript{34}

- Sites that fail to account for changes in their practices may have to segregate new data from information collected under old policies where adequate permission was not obtained or disclosures provided.

- Simply stating in a privacy policy that a site’s practices may change or that the policy may be revised at any time is unlikely to be viewed as satisfactory by the FTC or state courts where practices inconsistent with policies in force at the time information was collected are likely to be challenged.\textsuperscript{35}
  - How will data collected under prior policies be treated?
  - How will notice of the new policy be given to users?

- What mechanism has been adopted to provide notice of policy revisions?
  - Some sites notify users by email or post notices prominently on their homepages.\textsuperscript{36}
  - Cookie files may be used to ensure that users have been notified of (or, where required, given consent to) policy revisions.
  - Registered users should be given notice when they first log-on after a new policy has been posted
  - Problems may arise if later practices are inconsistent with commitments made at the time information was collected.

**Internal Implementation**

- Have adequate internal record-keeping procedures

\textsuperscript{34}See supra § 26.13[6] (California law); see also supra § 26.13[5][C] (discussing the FTC’s position on material changes).

\textsuperscript{35}Businesses generally must comply with the laws in effect in all fifty states and possibly multiple countries (unless they affirmatively block orders or access from residents of particular jurisdictions or otherwise take measures to limit the scope of regulatory and judicial jurisdiction). See infra chapters 36, 52 to 54. Thus, although particular practices are likely to be deemed appropriate by a majority of courts, privacy statements often are drafted in light of the risk of liability presented by any single jurisdiction.

\textsuperscript{36}The issues surrounding updating contracts and policies are analyzed in section 22.04.
been established to ensure that adequate documentation exists of the particular version of the policy in effect on a given date, in the event of litigation or a regulatory action?

- Have adequate internal (and possibly external) compliance procedures been put in place to ensure that employees are educated about the company's obligations under the policy and assure that the policy in fact is followed?
- Have adequate contract administration procedures been adopted to ensure that third-party contracts comply with California and other state laws (if personally identifying information is to be transferred to third parties)?
- Have adequate procedures been put in place to conduct periodic privacy and security audits to ensure the continued accuracy of the policy (and make appropriate adjustments or revisions over time)?
- What internal mechanisms have been put in place to ensure that the policy is revised as practices change? Will the Legal Department receive notice when new marketing, business practices or technologies are implemented?

## 26.15 Class Action Litigation

Since 2010, there has been an explosion of data privacy-related putative class action suits filed against Internet companies, social networks, social gaming sites, advertising companies, application providers, mobile device distributors, and companies that (regardless of the nature of their business) merely advertise on the Internet, among others. While data privacy class actions have been brought since the 1990s, the dramatic increase in suits filed beginning in 2010 largely results from increased attention given to data privacy in Washington during the early years of the Obama Administration, including Congressional hearings and talk of potential consumer privacy legislation, the FTC’s ongoing focus on behavioral advertising, and publicity about the settlement of two high profile putative class action suits where defendants paid large sums at the very outset of each case without engaging in significant litigation. All of these developments,

---

37See supra § 26.13[6].
E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS, 2D 2014
Ian C. Ballon

A business-oriented Treatise from a leading Internet litigator
TAKE YOUR INTERNET AND MOBILE PRACTICE TO THE NEXT LEVEL

E-Commerce & Internet Law is a comprehensive, authoritative work covering business-to-business and business-to-customer issues, regulatory issues, and emerging trends. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to more than hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into four sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Privacy, Security and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Liability of Internet Sites and Services (Including Social Networks and Blogs)
- Civil Jurisdiction and Litigation

Questions to Answer as Internet law moves to mobile devices, social media and the cloud:

- Does content syndication to mobile providers take a service provider outside the DMCA?
- How does text marketing differ from email marketing?
- Privacy issues when dealing with users who are subject to COPPA or teenagers not subject to COPPA but subject to heightened concern
- Facebook and Twitter contacts as the basis for personal jurisdiction
- How to obtain substitute service over a foreign defendant in an Internet dispute

Key Features of E-Commerce & Internet Law

- The only treatise to comprehensively and exhaustively cover the liability of Internet service providers, cloud storage providers, bloggers, and owners and operators of social networks and other Web 2.0 applications
- Substantial caselaw coverage on Terms of Use and Internet contracts to help you draft better agreements, with sample forms and provisions
- Latest caselaw and analysis on sponsored links, key word sales, and liability for search engine optimization practices
- Includes coverage on enforcing judgments against domain names and the extent to which even unrelated claims against foreign defendants could be satisfied in U.S. courts
- Rethinking consumer criticism, gripe site, blog, and fan site law in light of new Lanham Act and CDA caselaw (including a checklist for evaluating potential claims and their viability)
- Comprehensive analysis of state law security breach notification statutes, together with practical tips on how to prepare for and respond to security breaches
- Extensive data on the prices paid for domain names and how to value them
- How to draft Privacy Policies, Terms of Use, and other documents and conduct website and privacy audits
- Practical tips, checklists, forms, and helpful information that goes well beyond what is usually included in a legal treatise
- Glossary terms drawn from the latest caselaw (helpful for briefs and contract definitions)
- Practical strategies for effectively documenting Internet transactions, drafting forms, and devising winning litigation strategies
- Exhaustive DMCA guidelines, CDA analysis, and strategies for managing user content
- Most thorough and clear cut analysis of Internet jurisdiction available anywhere
- Clear, concise, comprehensive and practical analysis

To order call 1-888-728-7677
or visit legalsolutions.thomsonreuters.com
Part I. Sources of Internet Law and Practice: A Framework for Developing New Law

Chapter 1. Context for Developing the Law of the Internet

2. A Framework for Developing New Law
3. Using the Internet in Your Legal Practice: Online Resources and Strategies

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Database Protection and Screen Scaring
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names
8. Internet Patents

Part III. Licenses and Contracts

14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: UCITA, the UETA, Federal Legislation and the EU Distance Sales Directive
16. Internet Licenses: Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements
24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements

Part IV. Privacy, Security and Internet Advertising

25. Introduction to Consumer Protection in Cyberspace
26. Data Privacy

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. Taxation of Electronic Commerce
34. Antitrust Restrictions on the Conduct of Electronic Commerce
35. State and Local Regulation of the Internet

Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption

37. Defamation, Torts and the Good Samaritan Exemption
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression In Cyberspace

Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children

Chapter 40. Child Pornography and Obscenity
41. Laws Regulating Non-Obscene Adult Content Directed at Children
42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

Part VIII. Theft of Digital Information and Related Internet Crimes

43. Detecting and Retrieving Stolen Corporate Data
44. Criminal and Related Civil Remedies for Software and Digital Information Theft
45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email
46. Identity Theft
47. Civil Remedies for Unlawful Seizures

Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)

48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Website Owner and Service Provider Liability for User Generated Content and User Misconduct
50. Strategies for Managing Third-Party Liability Risks
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites

Part X. Civil Jurisdiction and Litigation

52. General Overview of Cyberspace Jurisdiction
53. Personal Jurisdiction in Cyberspace
54. Venue and the Doctrine of Forum Non Conveniens
55. Choice of Law in Cyberspace
56. Internet ADR
57. Internet Litigation
58. Email and other Electronic Communications in Litigation and in Corporate and Employer Policies
59. Use of Email in Attorney-Client

“Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet.”
Jay Monahan
Deputy General Counsel, Zynga, Inc.
> Practical analysis by a well-known litigator, including how contracts and Terms of Use in fact are construed in litigation

> New in-depth analysis of the safe harbor and anti-circumvention provisions of the Digital Millennium Copyright Act 15 years after its enactment

> Licensing music and user generated content online

> Clear, simple, understandable guidelines for making sense of the Electronic Communications Privacy Act, the Digital Millennium Copyright Act, the CAN-SPAM Act, the Computer Fraud and Abuse Act and others, with exhaustive case citations and practical explanations.

> Easy-to-use integrated COPPA analysis combining the statute, implementing regulations and FTC guidelines and commentary, extensively annotated for ease of use

> Mobile and Internet contracting with minors (and what age actually constitutes the age of majority)

> Comprehensive coverage of state laws limiting employer access to social media credentials, including copies of all state statutes

> Updated sample consumer arbitration agreement, accounting for the latest case law.

> Circuit splits and differences among state laws governing the Internet and e- and mobile commerce

> The first sale doctrine and why John Wiley & Sons, Inc. v. Kirtsaeng, 133 S. Ct. 1351 (2013) doesn’t fully resolve the issue of what constitutes a first sale in digital, virtual and other intangible goods

> Judicial confusion over so-called clickwrap and browsewrap agreements and what it means for your clients

> Fair use in social media and in connection with e-commerce and gripe sites

> Most comprehensive collection and analysis of data privacy, Internet security and behavioral advertising class action decisions available anywhere

> New section on TCPA litigation and the latest FTC regulations governing commercial text messaging

> Exhaustive analysis of database and website protection, screen scraping and the interplay between trespass, Computer Fraud and Abuse Act, copyright, conversion, trademark and other laws that may restrict use of material found online

> Understanding the interplay between new technologies and copyright inducement – and open and emerging areas in digital copyright law.

> New case law on cloud storage, infringement and privacy and security issues

> Latest trends involving privacy troll and spam troll litigation

> The statutory framework under ECPA and state law for obtaining and using evidence from social media, Internet and mobile sites and services – and what type of communications may not be obtained by civil subpoena

> Search engine optimization, embeds, in-line links, thumbnail images and favicons

> BitTorrent swarm cases and related joinder issues

> eDiscovery and electronic evidence spoliation

> Most comprehensive analysis available anywhere on the nature of exclusive rights on the Internet and personal jurisdiction law

> Investor and owner liability for allegedly infringing technologies and business models – updated for all the latest case law through 2013!

> A litigator’s perspective on online contract formation, unconscionability, illusory agreements and contracts and licenses generally

SAVE 20% NOW!!
To order call 1-888-728-7677 or visit legalsolutions.thomsonreuters.com, enter promo code WPD20 at checkout

List Price: $1,479
Discounted Price: $1,183.20